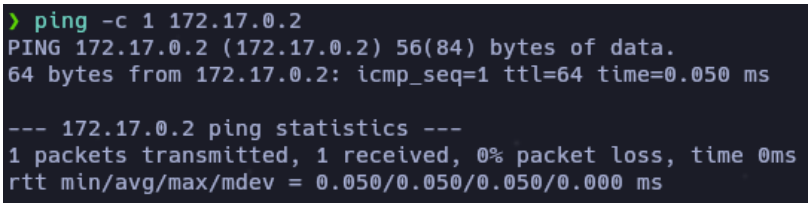
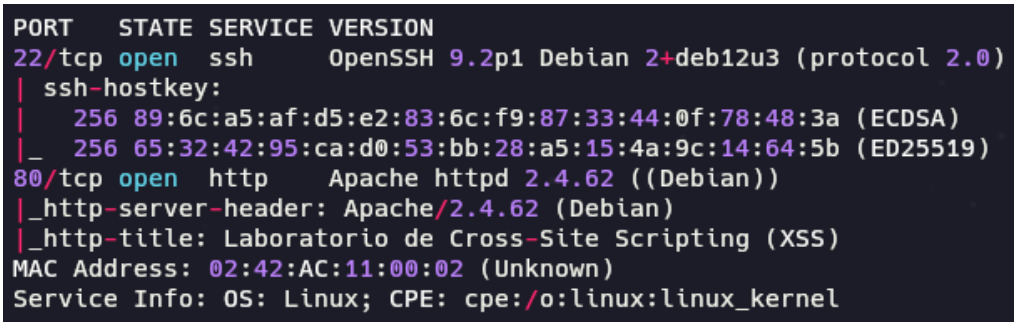
Desplegamos la máquina.


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

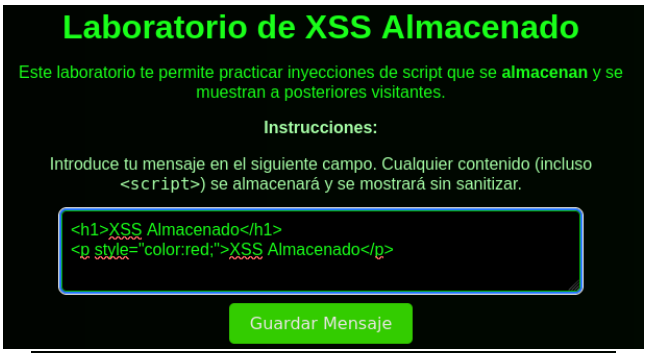


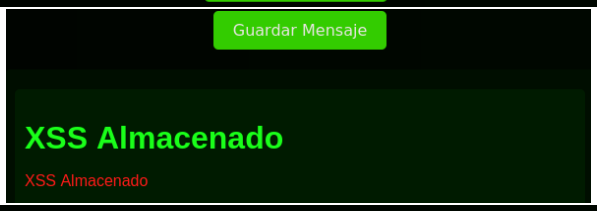

Con nmap vemos los puertos que están abiertos y sus servicios.

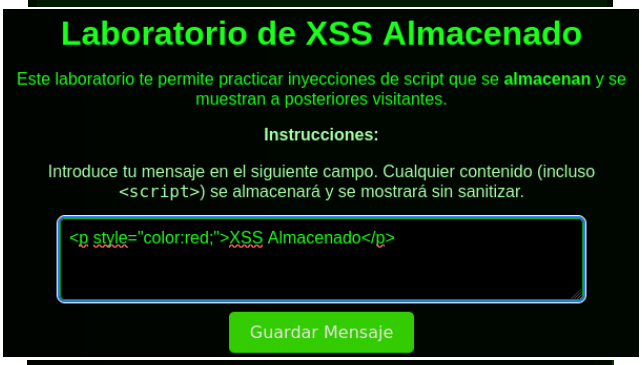


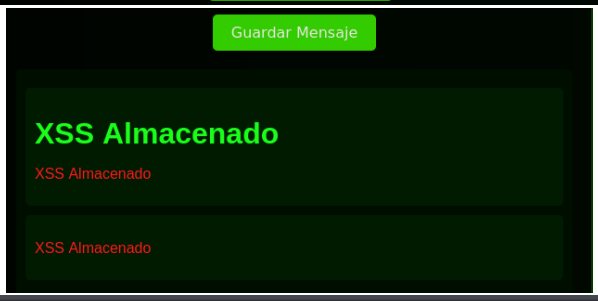

Vamos a realizar los 3 laboratorios que nos indican. El primero es un XSS reflected.

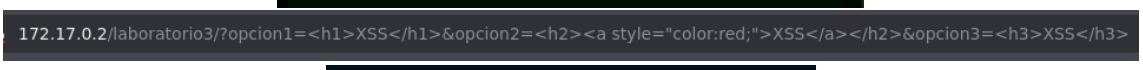
El segundo es un XSS stored.

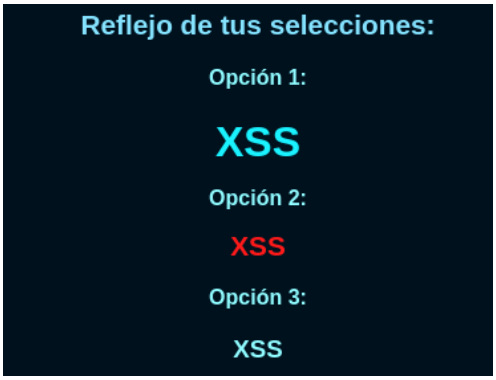


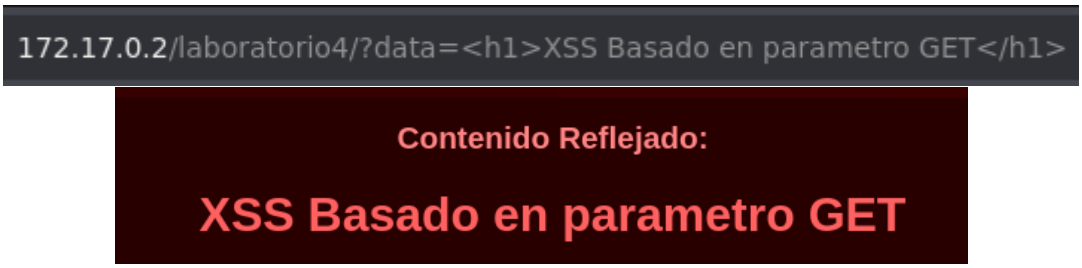



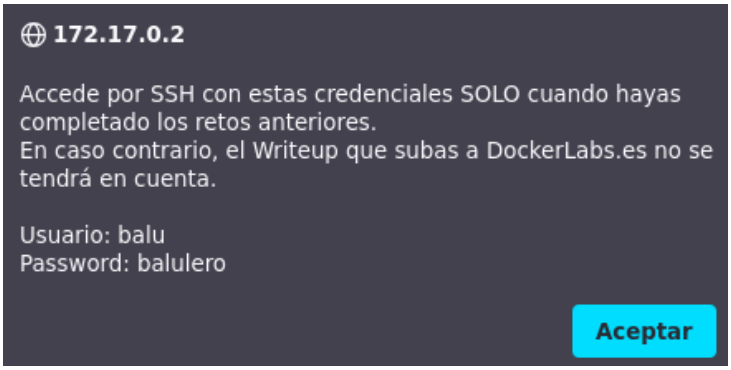



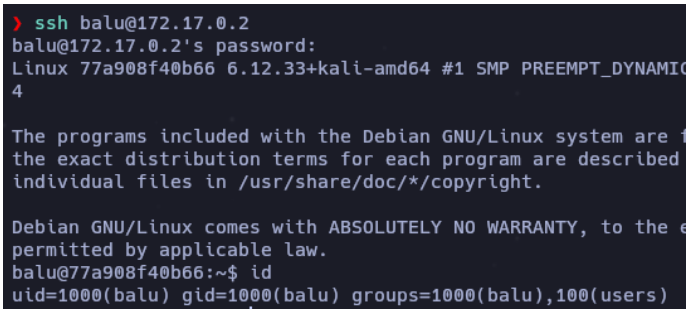
El tercero es XSS basado en GET.



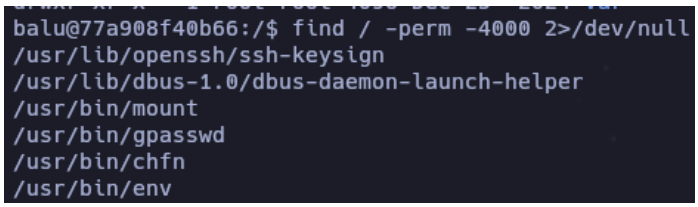

Una vez completados los 3 laboratorios vemos que tenemos un usuario y contraseña con el que podemos acceder mediante ssh.




Nos conectamos a la máquina por ssh.




Vemos que tiene un binario env con permisos SUID.




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